The specifications and information regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

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

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

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

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

© 2013 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xxvii
  Purpose xxvii
  Audience xxviii
  Organization xxviii
  Related documentation xxix
  Conventions xxx
  Obtain documentation and submit service request xxxi
  Cisco product security overview xxxi

PART I Cisco Unified Communications Manager 1

CHAPTER 1 Introduction 3
  About Cisco Unified Communications Manager 3
  Key features and benefits 4
  Cisco Unified Communications Manager Administration web browsers 4
    Web browser support 4
    Log into Cisco Unified Communications Manager Administration 5
    Log out of Cisco Unified Communications Manager Administration 6
    Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS) support 6
    Web interface timeout 7
      Import Cisco certificate for Internet Explorer 7 7
      Import Cisco certificate for Internet Explorer 8 8
      Import Cisco certificate for FireFox 3.x 10
      Import Cisco certificate for Safari 4.x 11
      Copy web browser certificates to file 12
      Copy FireFox certificate to file 13
    Cisco Unified Communications Manager Administration application 14
Cisco Unified Communications Manager Administration Graphical User Interface 14
  Navigation drop-down list box 14
  Links to Search documentation, About, and Logout 15
  Menu bar 15
  Shared login 15
Cisco Unified Communications Manager Administration Help 16
  Find and delete records 16
  Add and copy records 17
  GUI buttons and icons 18
    Find and List Window buttons and icons 19
    Configuration windows buttons and icons 20
Cisco Unified Presence server access 20
Clustered Cisco Unified Presence server access 21
Login message customization 21
Last successful login message 21
Accessibility 21
  Access icons 21
  Access buttons 22
Where to find more information 22

PART II

System setup 23

CHAPTER 2

Server setup 25
  About server setup 25
  Server deletion 26
  Add node to cluster before install 27
  Add deleted server back in to cluster 28
  Server settings 29
  View Presence Server Status 31

CHAPTER 3

Cisco Unified Communications Manager setup 33
  About Cisco Unified Communications Manager setup 33
  Cisco Unified Communications Manager settings 33
  Synchronize Cisco Unified Communications Manager with devices 37
  Activate Cisco CallManager service 37
Deactivate Cisco CallManager service 38

## CHAPTER 4
Cisco Unified Communications Manager group setup 39
- About Cisco Unified Communications Manager group setup 39
- Cisco Unified Communications Manager group deletion 40
- Cisco Unified Communications Manager group settings 40
- Synchronize Cisco Unified Communications Manager Group settings with devices 42

## CHAPTER 5
Phone NTP reference setup 43
- About phone NTP reference setup 43
- Phone NTP reference deletion 44
- Phone NTP reference settings 44

## CHAPTER 6
Date and time group setup 47
- About date and time group setup 47
- Add phone NTP reference to SIP phones in date and time group 48
- Date and time group deletion 49
- Date and time group settings 49
- Synchronize date and time group settings with devices 50

## CHAPTER 7
Region setup 53
- Audio Codec Preference list 53
- Create new Audio Codec Preference list 54
- Edit Audio Codec Preference list 54
- Delete Audio Codec Preference list 55
- About region setup 55
- Set up regions 56
- Region deletion 57
- Audio and video call bit rate settings 57
- Synchronize region settings with devices 61

## CHAPTER 8
Device pool setup 63
- About device pool setup 63
- Device pool deletion 64
- Device pool settings 64
Synchronize device pool settings with devices  79

<table>
<thead>
<tr>
<th><strong>CHAPTER 9</strong></th>
<th>DHCP server setup  81</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About DHCP server setup  81</td>
</tr>
<tr>
<td></td>
<td>DHCP server deletion  81</td>
</tr>
<tr>
<td></td>
<td>DHCP server settings  81</td>
</tr>
<tr>
<td></td>
<td>Activate DHCP monitor service  83</td>
</tr>
<tr>
<td></td>
<td>Start DHCP monitor service  83</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CHAPTER 10</strong></th>
<th>DHCP subnet setup  85</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About DHCP subnet setup  85</td>
</tr>
<tr>
<td></td>
<td>DHCP subnet deletion  85</td>
</tr>
<tr>
<td></td>
<td>DHCP subnet settings  85</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CHAPTER 11</strong></th>
<th>LDAP system setup  89</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About LDAP System setup  89</td>
</tr>
<tr>
<td></td>
<td>LDAP system settings  90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CHAPTER 12</strong></th>
<th>LDAP directory setup  93</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About LDAP directory setup  93</td>
</tr>
<tr>
<td></td>
<td>LDAP directory settings  94</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CHAPTER 13</strong></th>
<th>LDAP authentication setup  101</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About LDAP authentication setup  101</td>
</tr>
<tr>
<td></td>
<td>Update LDAP authentication  102</td>
</tr>
<tr>
<td></td>
<td>LDAP authentication settings  102</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CHAPTER 14</strong></th>
<th>LDAP custom filter setup  105</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About LDAP custom filter setup  105</td>
</tr>
<tr>
<td></td>
<td>LDAP filter deletion  106</td>
</tr>
<tr>
<td></td>
<td>LDAP filter settings  106</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CHAPTER 15</strong></th>
<th>Location setup  107</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About location setup  107</td>
</tr>
<tr>
<td></td>
<td>Location deletion  108</td>
</tr>
</tbody>
</table>
Location settings 109
Location Bandwidth Manager Group 113
Location Bandwidth Manager Intercluster Replication Group Settings 114

CHAPTER 16
Survivable remote site telephony setup 115
  About SRST reference setup 115
  SRST reference deletion 115
  SRST reference settings 116

CHAPTER 17
MLPP Domain setup 119
  About MLPP Domain Setup 119
  MLPP domain deletion 119
  MLPP domain settings 120

CHAPTER 18
Resource Priority Namespace Network Domain setup 121
  About Resource Priority Namespace Network Domain setup 121
  Resource Priority Namespace Network Domain deletion 122
  Resource Priority Namespace Network Domain settings 122

CHAPTER 19
Resource Priority Namespace List setup 123
  About Resource Priority Namespace List setup 123
  Resource Priority Namespace List deletion 123
  Resource Priority Namespace List settings 124

CHAPTER 20
E911 messages 125
  E911 messages setup 125
  Set up E911 Messages 125

CHAPTER 21
Enterprise parameter setup 127
  About enterprise parameter setup 127
  Update enterprise parameters 128
  Synchronize enterprise parameters with devices 128

CHAPTER 22
Enterprise phone setup 129
  Set up enterprise phone parameters 129
ROUTE GROUP SETTINGs 178
Add devices to route group 180
Remove devices from route group 181

Chapter 33
Route list setup 183
About route list setup 183
Route list deletion 184
Route list settings 184
Add route groups to route list 185
Remove route groups from route list 187
Change route group order in route list 187
Synchronize route list settings with route groups 188

Chapter 34
Route pattern setup 189
About route pattern setup 189
Route pattern settings 190

Chapter 35
Line group setup 201
About line group setup 201
Line group deletion 202
Line group settings 202
Add members to line group 207
Remove members from line group 207

Chapter 36
Hunt list setup 209
About Hunt List configuration 209
Find hunt lists 210
Add hunt list 210
Add line groups to hunt list 211
Remove line groups from hunt list 212
Change line groups order in hunt list 213
Synchronize hunt list settings with line groups 213
Delete hunt list 214

Chapter 37
Hunt pilot setup 215
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>SIP route pattern setup</td>
<td>227</td>
</tr>
<tr>
<td></td>
<td>About SIP route pattern setup</td>
<td>227</td>
</tr>
<tr>
<td></td>
<td>SIP route pattern deletion</td>
<td>228</td>
</tr>
<tr>
<td></td>
<td>SIP route pattern settings</td>
<td>228</td>
</tr>
<tr>
<td>39</td>
<td>Time period setup</td>
<td>233</td>
</tr>
<tr>
<td></td>
<td>About time period setup</td>
<td>233</td>
</tr>
<tr>
<td></td>
<td>Time period deletions</td>
<td>233</td>
</tr>
<tr>
<td></td>
<td>Time period settings</td>
<td>234</td>
</tr>
<tr>
<td>40</td>
<td>Time schedule setup</td>
<td>237</td>
</tr>
<tr>
<td></td>
<td>About time schedule setup</td>
<td>237</td>
</tr>
<tr>
<td></td>
<td>Time schedule deletions</td>
<td>237</td>
</tr>
<tr>
<td></td>
<td>Time schedule settings</td>
<td>238</td>
</tr>
<tr>
<td>41</td>
<td>Partition setup</td>
<td>241</td>
</tr>
<tr>
<td></td>
<td>About partition setup</td>
<td>241</td>
</tr>
<tr>
<td></td>
<td>Partition deletions</td>
<td>242</td>
</tr>
<tr>
<td></td>
<td>Partition settings</td>
<td>242</td>
</tr>
<tr>
<td></td>
<td>Search for partition</td>
<td>244</td>
</tr>
<tr>
<td></td>
<td>Synchronize partition settings with devices</td>
<td>244</td>
</tr>
<tr>
<td>42</td>
<td>Calling search space setup</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>About calling search space setup</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>Calling search space deletions</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>Calling search space settings</td>
<td>248</td>
</tr>
<tr>
<td>43</td>
<td>Translation pattern setup</td>
<td>251</td>
</tr>
<tr>
<td></td>
<td>About translation pattern setup</td>
<td>251</td>
</tr>
<tr>
<td></td>
<td>Translation pattern deletions</td>
<td>252</td>
</tr>
<tr>
<td></td>
<td>Translation pattern settings</td>
<td>252</td>
</tr>
</tbody>
</table>
CHAPTER 44 Directory number setup 263
   About directory number setup 263
   Directory number settings 265
      Display calling search space 291
   Synchronize directory number settings with devices 292
   Set up Private Line Automatic Ringdown (PLAR) 293
      Set up PLAR example 293
   Remove directory number from phone 294
   Create Cisco Unity Connection voice mailbox 295

CHAPTER 45 Meet-Me number and pattern setup 297
   About Meet-Me number and pattern setup 297
   Meet-Me number and pattern settings 297

CHAPTER 46 Dial plan installer 299
   Dial plan setup 299
   Edit dial plan 299
      Install dial plan on Cisco Unified Communications Manager 300
      Set up route pattern details for non-NANP dial plan 301
      Upgrade dial plan 301
      Uninstall dial plan 302
   Restart Cisco CallManager service 303

CHAPTER 47 Route plan report 305
   About route plan report 305
   View route plan records 306
   Delete unassigned directory number 307
   Update unassigned directory numbers 308
   View route plan reports in files 308

CHAPTER 48 Calling party transformation pattern setup 311
   About calling party transformation pattern setup 311
   Calling party transformation pattern settings 311
CHAPTER 49
Called party transformation pattern setup 315
   About called party transformation pattern setup 315
   Called party transformation pattern settings 315

CHAPTER 50
Intercluster directory URI 319
   Intercluster directory URI settings 319
   Imported directory URI catalog settings 320
   Find imported directory URIs 321
   Import Directory URIs from a non-ILS system 322
   Directory URI format 323

CHAPTER 51
Other call routing menu options 325
   Intercom partition setup 325
   Intercom calling search space setup 326
   Intercom directory number setup 326
   Intercom translation pattern setup 326
   Access list setup 326
   Client Matter Code setup 327
   Forced Authorization Code setup 327
   Call Park setup 327
   Directed Call Park setup 328
   Call Pickup Group setup 328
   Transformation profile setup 329
   Mobility setup 329
   Logical partitioning policy setup 329
   Call control discovery setup 330
   External call control profile setup 330

PART IV
Media resource setup 331

CHAPTER 52
Annunciator setup 333
   About annunciator setup 333
   Annunciator deletion 334
   Annunciator settings 334
CHAPTER 53  Conference Bridge setup  337

About conference bridge setup  337
Conference Bridge deletion  338
Conference Bridge settings  338
  Software Conference Bridge settings  339
  Hardware Conference Bridge settings  341
  Cisco IOS Conference Bridge settings  343
  Cisco Video Conference Bridge settings  345
  Cisco Conference Bridge (WS-SVC-CMM) settings  348
  Cisco IOS Heterogeneous Video Conference Bridge settings  350
  Cisco IOS Guaranteed Audio Video Conference Bridge settings  352
  Cisco IOS Homogeneous Video Conference Bridge settings  354
  Cisco TelePresence MCU settings  355
  CSCub65671 Route Class Configuration SIP Information  359

Set up TLS connection with Cisco TelePresence MCU  360
Synchronize conference device settings  361

CHAPTER 54  Media termination point setup  363

About media termination point setup  363
Cisco IOS media termination point setup  364
Cisco IOS media termination point deletion  364
Cisco IOS media termination point settings  365
Synchronize media termination point  365

CHAPTER 55  Transcoder setup  367

About transcoder setup  367
Transcoder deletion  367
Transcoder settings  368
Synchronize transcoder  369

CHAPTER 56  Media resource group setup  371

About media resource group setup  371
Media resource group deletion  372
<table>
<thead>
<tr>
<th>Chapter 57</th>
<th>Media resource group list setup 375</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About media resource group list setup 375</td>
</tr>
<tr>
<td></td>
<td>Media resource group list deletion 375</td>
</tr>
<tr>
<td></td>
<td>Media resource group list settings 376</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 58</th>
<th>Announcement setup 377</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco-provided announcements and tones 377</td>
</tr>
<tr>
<td></td>
<td>About announcement setup 378</td>
</tr>
<tr>
<td></td>
<td>Announcement deletions 379</td>
</tr>
<tr>
<td></td>
<td>Announcement settings 379</td>
</tr>
<tr>
<td></td>
<td>Announcements in the Find and List Announcements Window 380</td>
</tr>
<tr>
<td></td>
<td>Upload customized announcement 381</td>
</tr>
<tr>
<td></td>
<td>Play announcement 382</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 59</th>
<th>Other media resource menu options 383</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Music On Hold audio source setup 383</td>
</tr>
<tr>
<td></td>
<td>Fixed MOH audio source setup 383</td>
</tr>
<tr>
<td></td>
<td>Music On Hold server setup 384</td>
</tr>
<tr>
<td></td>
<td>MOH audio file management setup 384</td>
</tr>
<tr>
<td></td>
<td>Mobile voice access setup 384</td>
</tr>
</tbody>
</table>

| Part V     | Advanced features setup 385 |

<table>
<thead>
<tr>
<th>Chapter 60</th>
<th>Cisco voice-mail port setup 387</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About Cisco voice-mail port setup 387</td>
</tr>
<tr>
<td></td>
<td>Cisco voice-mail port deletion 388</td>
</tr>
<tr>
<td></td>
<td>Cisco voice-mail port settings 388</td>
</tr>
<tr>
<td></td>
<td>Synchronize Cisco voice-mail port with devices 393</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 61</th>
<th>Cisco Voice Mail Port Wizard 395</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Voice-mail port setup using wizard 395</td>
</tr>
<tr>
<td></td>
<td>Add new Cisco voice-mail server and ports using wizard 396</td>
</tr>
<tr>
<td></td>
<td>Voice Mail Port Wizard device information setup 397</td>
</tr>
</tbody>
</table>
Add BRI port to MGCP gateway 528
Add Cisco IOS SCCP gateway 529
Add non-IOS MGCP gateway 530
Add Cisco IOS H.323 gateway 531
Add analog access gateway and ports 532
Add Cisco VG248 analog phone gateway 532
Gateway and port modification 534
Synchronize gateway 534
Update gateways and ports 534

CHAPTER 69  Cisco Unified IP Phone setup 537
About Cisco Unified IP Phones and device setup 538
Phone setup 539
Phone deletion preparation 540
Phone settings 541
Phone settings migration 570
Speed-dial and abbreviated-dial setup 570
BLF speed dial setup 576
BLF directed Call Park setup 576
Set up Cisco Unified IP Phone 577
Migrate existing phone settings to another phone 579
    Phone migration settings 580
Synchronize phone 581
Set up speed-dial buttons or abbreviated dialing 582
Set up IP phone services 583
    Subscribe to service 583
    Update service 584
    Unsubscribe from service 584
Service URL button setup 585
    Add service URL button 585
Copy phone record to remote destination profile 586
Modify custom phone button template button items 587
Find actively logged-in device 588
Find remotely logged-in device 589
Display phone MAC address 590
CHAPTER 76  Softkey template setup  675
About softkey template setup  675
Find softkey template  675
Create nonstandard softkey templates  676
Add application softkeys to nonstandard softkey templates  677
Set up softkey positions in nonstandard softkey templates  678
Softkey template modification  679
  Rename softkey template  679
  Delete softkey template  680
  Update softkey template  681
  Synchronize softkey template settings with devices  681
IP phone softkey template assignment  682

CHAPTER 77  IP phone services setup  683
About IP phone service setup  683
IP phone service deletion  684
IP phone service settings  685
IP phone service parameter settings  688
  Cisco-provided default IP phone services  689
Set up IP phone service parameters  691
IP phone service parameter deletion  692
Add IP phone services to phone buttons  693

CHAPTER 78  SIP profile setup  695
About SIP profile setup  695
SIP profile reset  695
SIP profile deletion  695
SIP profile settings  696
Synchronize SIP profile settings with SIP devices  711

CHAPTER 79  Common device setup  713
About common device setup  713
Common device setup deletion  713
Common device settings  714
Synchronize common device settings with devices 719

CHAPTER 80

Common phone profile setup 721
About common phone profile setup 721
Common phone profile deletion 721
Common phone profile settings 722
Synchronize common phone profile settings with devices 725

CHAPTER 81

Feature Control Policy setup 727
About Feature Control Policy setup 727
Feature Control Policy deletion 728
Feature Control Policy settings 729
Feature Control Policy default values 729

CHAPTER 82

Recording Profile setup 731
About Recording Profile setup 731
Recording profile deletion 731
Recording profile settings 732

CHAPTER 83

SIP normalization script setup 733
About SIP normalization script setup 733
SIP normalization script deletion 734
SIP normalization script settings 734
Import SIP normalization script 737

CHAPTER 84

Other device menu options 739
Remote destination setup 739
Remote destination profile setup 739

PART VII

Application setup 741

CHAPTER 85

Cisco Unified Communications Manager Assistant Configuration Wizard 743

CHAPTER 86

Plug-in setup 745
Update plugin URL settings 745
Install plug-ins  746
Update plugin URL  746

PART VIII  User management setup  749

CHAPTER 87  Credential policy default setup  751
   About credential policy default setup  751
   Credential policy default settings  752
   Assign and set up credential policy defaults  753

CHAPTER 88  Credential policy setup  755
   About credential policy setup  755
   Credential policy deletion  756
   Credential policy settings  757

CHAPTER 89  Application user setup  759
   About application user setup  759
   Add application user  760
   Application user deletion  761
   Application user settings  761
   Add administrator user to Cisco Unity or Cisco Unity Connection  765
   Change application user password  767
   Manage application user credential information  767
   Credential settings and fields  768
   Associate devices to application users  769

CHAPTER 90  End user setup  771
   About end user setup  771
   End user deletion  772
   End user settings  773
   Create Cisco Unity Connection voice mailbox  779
   Change end user password  781
   Change end user PIN  781
   Manage end user credential information  782
   Credential settings and fields  782
Set up end user information 784
Associate devices to end user 785
Associate Cisco Extension Mobility profile to Cisco Unified IP Phone 786

CHAPTER 91  
Role setup 787
Role setup 787
Example add or copy roles 788
Role deletions 788
Role settings 788

CHAPTER 92  
Access control group setup 791
About access control group setup 791
Reduced permissions for Access Control Groups 791
Find access control group 792
Set up access control group 793
Delete access control group 794
Add users to access control groups 794
Delete users from access control groups 796
Assign roles to access control group 796
View user roles, access control groups, and permissions 797

CHAPTER 93  
End user phone addition 799
About end user phone and device addition 799
User and device settings 800
Add and associate end user and phone 802

CHAPTER 94  
UC service setup 803
About UC service setup 803
Add voicemail service 804
Add mailstore service 805
Add conferencing service 807
Add directory service 809
Add IM and Presence service 811
Add CTI service 812
Enable digest authentication for third-party SIP phones 880
DTMF reception 881
Licensing third-party SIP phones 881
Where to find more information 882

APPENDIX C

AS-SIP configuration 885
AS-SIP capabilities 886
Set up AS-SIP line endpoints 886
Configuration differences for phones running AS-SIP 887
AS-SIP conferencing 888
Unified Communications Manager identification of third-party phones 889
Third-party phones running AS-SIP 889
End user configuration settings 889
SIP profile configuration settings 890
Require DTMF reception 891
Set up phone security profile settings 891
Set up TLS 891
Add and configure third-party phones 891
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:


- Purpose, page xxvii
- Audience, page xxviii
- Organization, page xxviii
- Related documentation, page xxix
- Conventions, page xxx
- Obtain documentation and submit service request, page xxxi
- Cisco product security overview, page xxxi

Purpose

The Cisco Unified Communications Manager Administration Guide provides instructions for administering the Cisco Unified Communications Manager (formerly Cisco Unified CallManager) system. This guide includes descriptions of procedural tasks that you complete by using Cisco Unified Communications Manager Administration. The Cisco Unified Communications Manager Administration Guide also provides references for commands to assist you in using Cisco Unified Communications Manager. This book acts as a companion to the Cisco Unified Communications Manager System Guide, which provides conceptual information about Cisco Unified Communications Manager and its components as well as tips for setting up features by using Cisco Unified Communications Manager Administration.
Audience

The *Cisco Unified Communications Manager Administration 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 the organization of this guide.

<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1</td>
<td>&quot;Cisco Unified Communications Manager&quot;</td>
</tr>
<tr>
<td></td>
<td>Contains information about general topics that are related to the configuration and operation of Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Part 2</td>
<td>&quot;System Configuration&quot;</td>
</tr>
<tr>
<td></td>
<td>Contains information on how to configure the items in the Cisco Unified Communications Manager Administration System menu.</td>
</tr>
<tr>
<td>Part 3</td>
<td>&quot;Call Routing Configuration&quot;</td>
</tr>
<tr>
<td></td>
<td>Contains information on how to configure call routing functions and features in Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td>Part 4</td>
<td>&quot;Media Resource Configuration&quot;</td>
</tr>
<tr>
<td></td>
<td>Contains information on how to configure media resources that are used in conjunction with Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Part 5</td>
<td>&quot;Advanced Features Configuration&quot;</td>
</tr>
<tr>
<td></td>
<td>Contains information on how to configure the following features in Cisco Unified Communications Manager Administration:</td>
</tr>
<tr>
<td></td>
<td>• Voice mail and messaging</td>
</tr>
<tr>
<td></td>
<td>• Service Advertisement Framework (SAF)</td>
</tr>
<tr>
<td></td>
<td>• Cisco Extension Mobility Cross Cluster (EMCC)</td>
</tr>
<tr>
<td></td>
<td>• Cisco Intercompany Media Engine</td>
</tr>
<tr>
<td></td>
<td>• Fallback</td>
</tr>
<tr>
<td></td>
<td>• Virtual Private Network (VPN)</td>
</tr>
<tr>
<td>Part 6</td>
<td>&quot;Device Configuration&quot;</td>
</tr>
<tr>
<td></td>
<td>Contains information on how to configure devices in Cisco Unified Communications Manager Administration.</td>
</tr>
</tbody>
</table>
### Related documentation

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

- Installing Cisco Unified Communications Manager Release 8.6(1)
- Upgrading Cisco Unified Communications Manager Release 8.6(1)
- Cisco Unified Communications Manager Documentation Guide
- Release Notes for Cisco Unified Communications Manager Release 8.6(1)
- Cisco Unified Communications Manager System Guide
- Cisco Unified Communications Manager Features and Services 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><strong>Convention</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface font</strong></td>
<td>Commands and keywords are in boldface.</td>
</tr>
<tr>
<td><strong>italic font</strong></td>
<td>Arguments for which you supply values are in italics.</td>
</tr>
<tr>
<td><strong>[ ]</strong></td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>**{ x</td>
<td>y</td>
</tr>
<tr>
<td>**[ x</td>
<td>y</td>
</tr>
<tr>
<td><strong>string</strong></td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>screen font</strong></td>
<td>Terminal sessions and information the system displays are in screen font.</td>
</tr>
<tr>
<td><strong>boldface screen font</strong></td>
<td>Information you must enter is in <strong>boldface screen</strong> font.</td>
</tr>
<tr>
<td><strong>italic screen font</strong></td>
<td>Arguments for which you supply values are in <strong>italic screen</strong> font.</td>
</tr>
<tr>
<td><strong>^</strong></td>
<td>The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td><strong>&lt; &gt;</strong></td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
</tbody>
</table>

Notes use the following conventions:

**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 conventions:

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.

Obtain documentation and submit 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.
PART I

Cisco Unified Communications Manager

- Introduction, page 3
About Cisco Unified Communications Manager

Cisco Unified Communications Manager (formerly Cisco Unified CallManager) serves as the software-based call-processing component of the Cisco Unified Communications family of products. A wide range of Cisco Media Convergence Servers provides high-availability server platforms for Cisco Unified Communications Manager call processing, services, and applications.

The Cisco Unified Communications Manager system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified Communications Manager open telephony application programming interface (API).

Cisco Unified Communications Manager provides signaling and call control services to Cisco integrated telephony applications as well as third-party applications. Cisco Unified Communications Manager performs the following primary functions:

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
• Operations, administration, maintenance, and provisioning (OAM&P)

• Programming interface to external voice-processing applications such as Cisco IP Communicator, Cisco Unified IP Interactive Voice Response (IP IVR).

Key features and benefits

The Cisco Unified Communications Manager system includes a suite of integrated voice applications that perform voice-conferencing and manual attendant console functions. This suite of voice applications means that no need exists for special-purpose voice-processing hardware. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways. Because Cisco Unified Communications Manager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform, thereby avoiding expensive hardware upgrade costs.

Distribution of Cisco Unified Communications Manager and all Cisco Unified IP Phones, gateways, and applications across an IP network provides a distributed, virtual telephony network. This architecture improves system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN link and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available.

A web-browsable interface to the configuration database provides the capability for remote device and system configuration. This interface also provides access to HTML-based online help for users and administrators. Cisco Unified Communications Manager, designed to work like an appliance, refers to the following functions:

• Cisco Unified Communications Manager servers can get preinstalled with software to ease customer and partner deployment and automatically search for updates and notify administrators when key security fixes and software upgrades are available for their system. This process comprises Electronic Software Upgrade Notification.

• You can upgrade Cisco Unified Communications Manager servers while they continue to process calls, so upgrades take place with minimal downtime.

• Cisco Unified Communications Manager supports the Asian and Middle Eastern markets by providing support for Unicode on higher resolution phone displays.

• Cisco Unified Communications Manager provides Fault, Configuration, Accounting, Performance, and Security (FCAPS).

Cisco Unified Communications Manager Administration web browsers

You access the Cisco Unified Communications Manager Administration program from a PC that is not the web server or has Cisco Unified Communications Manager installed. No browser software exists on the server.

Related Topics

Web browser support, on page 4

Web browser support

Cisco Unified Communications Manager Administration supports the following operating system browsers:
• On Microsoft Windows XP, Vista, and 7:
  • Microsoft Internet Explorer (IE) 8, IE 9
  • Mozilla Firefox 4.x, Firefox 10.x
  • Google Chrome 8.x (only User Options page)

• On Apple OS X and later:
  • Apple Safari 5.x
  • Firefox 4.x, 10.x
  • Chrome 8.x (only User Options page)

From any user PC in your network, browse into a server that is running Cisco Unified Communications Manager Administration and log in with administrative privileges.

**Note**
Simultaneous login to Cisco Unified Communications Manager Administration by a large number of users can cause performance to suffer. Try to limit the number of users and administrators that are logged on simultaneously.

**Note**
Cisco Unified Communications Manager Administration does not support the buttons in your browser. Do not use the browser buttons (for example, the Back button) when you perform configuration tasks.

**Related Topics**
Introduction, on page 3

**Log into Cisco Unified Communications Manager Administration**

Use the following procedure to log in to Cisco Unified Communications Manager Administration. 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 in the main window. For example, Cisco Unified Communications Manager may identify the following situations:

• Cisco Unified Communications Manager currently operates with starter (demo) licenses, so upload the appropriate license files.

• Cisco Unified Communications Manager currently operates with an insufficient number of licenses, so upload additional license files.

• 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.

Use the following procedure to browse into the server and log in to Cisco Unified Communications Manager Administration.
Procedure

Step 1  Start your preferred operating system browser.

Step 2  In the address bar of the web browser, enter the following case-sensitive URL:
https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do

where: <Unified CM-server-name> equals the name or IP address of the server

Note    You can optionally specify a port number.

Step 3  A Security Alert dialog box displays. Click the appropriate button.

Step 4  At the main Cisco Unified Communications Manager Administration window, enter the username and password that you specified during Cisco Unified Communications Manager installation and click Login. (If you want to clear the content of both fields, click Reset.)

Note    The window for entering username and password is not displayed if single sign-on is enabled for Cisco Unified Communications Manager Administration. For more information on single sign-on feature, see Single Sign On section in the Cisco Unified Communications Manager Features and Services Guide.

Note    For security purposes, Cisco Unified Communications Manager Administration logs you out after 30 minutes of inactivity, and you must log back in.

Log out of Cisco Unified Communications Manager Administration

Use the following procedure to log out of Cisco Unified Communications Manager Administration.

Procedure

Step 1  From the main Cisco Unified Communications Manager Administration window, click the Logout link in the upper, right corner.

Step 2  The window redisplays with the login fields.

Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS) support

HTTPS, or Hypertext Transfer Protocol over Secure Sockets Layer (SSL), secures communication between a browser and a web server for Microsoft Windows users. HTTPS uses certificates to ensure server identities and to secure the browser connection. HTTPS uses a public key to encrypt the data, including the user login and password, during transport over the Internet.

To enable HTTPS, you must download a certificate that identifies the server during the connection process. You can accept the server certificate for the current session only, or you can download the certificate to a trust folder (file) to secure the current session and future sessions with that server. The trust folder stores the certificates for all your trusted sites.

The following Cisco Unified Communications Manager applications support HTTPS: Cisco Unified Communications Manager Administration, Cisco Unity Connection Administration, Cisco Unified
Serviceability, the Cisco Unified CM User Options, Trace Collection Tool, the Real Time Monitoring Tool (RTMT), and the XML (AXL) application programming interface.

A self-signed certificate gets generated on the web server at installation (the certificate also gets migrated during upgrades).

Web interface timeout

Using the Command Line Interface (CLI), you can configure time, in minutes, after which the web interface times out and logs off the user. The default timeout value is 30 minutes. For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Import Cisco certificate for Internet Explorer 7

Internet Explorer (IE) 7 adds security features that change the way that the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Cisco Unified Communications Manager server, Internet Explorer 7 flags the Cisco Unified Communications Manager Administration website as untrusted and provides a certificate error, even when the trust store contains the server certificate.

Note

Cisco Unified Communications Manager Administration supports IE 7 when it is running on Microsoft Windows XP SP3.

Be sure to import the Cisco Unified Communications Manager certificate to Internet Explorer 7 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 7 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 7 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to the root certificate trust store for Internet Explorer 7.

Procedure

Step 1
Browse to the application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser). The browser displays a Certificate Error: Navigation Blocked page to indicate this website is untrusted.

Step 2
Click Continue to this website (not recommended) to access the server.
The Cisco Unified Communications Manager Administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3
To import the server certificate, click the Certificate Error status box to display the status report. Click the View Certificates link in the report.

Step 4
Verify the certificate details.
The Certification Path tab displays "This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store."
Step 5  Select the General tab in the Certificate window and click **Install Certificate**.
The Certificate Import Wizard launches.

Step 6  To start the Wizard, click **Next**.
The Certificate Store window displays.

Step 7  Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate
type, is selected and click **Next**.

Step 8  Verify the setting and click **Finish**.
A security warning displays for the import operation.

Step 9  To install the certificate, click **Yes**.
The Import Wizard displays “The import was successful.”

Step 10  Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate
window displays “This certificate is OK.”

Step 11  To verify that the trust store contains the imported certificate, click **Tools > Internet Options** in the Internet
Explorer toolbar and select the Content tab. Click **Certificates** and select the Trusted Root Certifications
Authorities tab. Scroll to find the imported certificate in the list.
After importing the certificate, the browser continues to display the address bar and a Certificate Error status
in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the
browser.

---

**What to Do Next**

You can copy the certificate to a file and store it locally so that you can restore the certificate whenever
necessary.

**Related Topics**

[Copy web browser certificates to file](#), on page 12

---

**Import Cisco certificate for Internet Explorer 8**

![Note](Note)

**Note**
Cisco Unified Communications Manager Administration supports IE 8 when it is running on Microsoft
Windows XP SP3 or Microsoft Vista SP2.

Be sure to import the Cisco Unified Communications Manager certificate to Internet Explorer 8 to secure
access without having to reload the certificate every time that you restart the browser. If you continue to a
website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 8 remembers
the certificate for the current session only.

After you download the server certificate, Internet Explorer 8 continues to display certificate errors for the
website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the
browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to
the root certificate trust store for Internet Explorer 8.
Procedure

Step 1 Browse to application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser). The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 Click Continue to this website (not recommended) to access the server. The Cisco Unified Communications Manager Administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the View Certificates link in the report.

Step 4 Verify the certificate details.


Step 6 To start the Wizard, click Next. The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click Next.

Step 8 Verify the setting and click Finish. A security warning displays for the import operation.

Step 9 To install the certificate, click Yes. The Import Wizard displays "The import was successful."

Step 10 Click OK. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click Tools > Internet Options in the Internet Explorer toolbar and select the Content tab. Click Certificates and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list. After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

What to Do Next

You can copy the certificate to a file and store it locally so that you can restore the certificate whenever necessary.

Related Topics

Copy web browser certificates to file, on page 12
Import Cisco certificate for FireFox 3.x

Note
Cisco Unified Communications Manager Administration supports FireFox 3.x when it is running on Microsoft Windows XP SP3, Microsoft Vista SP2 or Apple MAC OS X.

The first time that you (or a user) accesses Cisco Unified Communications Manager Administration or other Cisco Unified Communications Manager SSL-enabled virtual directories (after the Cisco Unified Communications Manager installation/upgrade) from a browser client, a Security Alert dialog box asks whether you trust the server.

When the dialog box displays, you must perform one of the following tasks:

• By clicking **I Understand The Risks**, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.

• By clicking **Get Me Out Of Here**, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click **I Understand The Risks**.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to the root certificate trust store for FireFox 3.x.

**Procedure**

---

**Step 1** Access the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

**Step 2** When the Security Alert dialog box displays, click **I Understand The Risks**.

**Step 3** Click **Add Exception**.

The Add Exception dialog box displays.

**Step 4** Click **Get Certificate**.

**Step 5** Check the Permanently store this exception check box.

**Step 6** Click **Confirm Security Exception**.

**Step 7** To view the details of the certificate by performing the following steps:

a) From the Firefox browser, click **Tools > Options**.

The Options dialog box displays.

b) Click **Advanced**.

c) Click **View Certificates**.

The Certificate Manager dialog box displays.

d) Highlight the certificate that you want to view and click **View**.

The Certificate Viewer dialog box displays.

e) Click the **Details** tab.

f) In the Certificate Fields field, highlight the field that you want to view.

Details display in the Field Values field.

g) From the Certificate Viewer dialog box, click **Close**.
h) From the Certificate Manager dialog box, click **OK**.

---

**Related Topics**

*Copy FireFox certificate to file,* on page 13

---

**Import Cisco certificate for Safari 4.x**

**Note**

Cisco Unified Communications Manager Administration supports Safari 4.x when it is running on Apple MAC OS X.

The first time that you (or a user) accesses Cisco Unified Communications Manager Administration or other Cisco Unified Communications Manager SSL-enabled virtual directories (after the Cisco Unified Communications Manager installation/upgrade) from a browser client, a Security Alert dialog box asks whether you trust the server.

When the dialog box displays, you must perform one of the following tasks:

- By clicking **Yes**, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.

- By clicking **Show Certificate > Install Certificate**, you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.

- By clicking **No**, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click **Yes** or install the certificate via the **Show Certificate > Install Certificate** options.

**Note**

The address that you use to access Cisco Unified Communications Manager must match the name on the certificate or a message will appear by default. If you access the web application by using the localhost or IP address after you install the certificate in the trusted folder, a security alert indicates that the name of the security certificate does not match the name of the site that you are accessing.

The following procedure describes how to import the Cisco Unified Communications Manager certificate to the root certificate trust store for Safari 4.x.

**Procedure**

**Step 1**

Access the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

**Step 2**

When the Security Alert dialog box displays, click **Show Certificate**.

You can click the Details tab to view the details of the certificate if you choose to verify the certificate data. To display a subset of settings, if available, choose one of the following options:
a) All—All options display in the Details pane.
b) Version 1 Fields Only—Version, Serial Number, Signature Algorithm, Issuer, Valid From, Valid To, Subject, and the Public Key options display.
c) Extensions Only—Subject Key Identifier, Key Usage, and the Enhanced Key Usage options display.
d) Critical Extensions Only—Critical Extensions, if any, display

e) Properties Only—Thumbprint algorithm and the thumbprint options display.

**Step 3** In the Certificate pane, click Install Certificate.
**Step 4** When the Certificate Import Wizard displays, click Next.
**Step 5** Click the **Place all certificates in the following store** radio button; click Browse.
**Step 6** Browse to Trusted Root Certification Authorities; select it and click OK.
**Step 7** Click Next.
**Step 8** Click Finish.
A Security Warning Box displays the certificate thumbprint for you.

**Step 9** To install the certificate, click Yes.
A message states that the import was successful. Click OK.

**Step 10** In the lower, right corner of the dialog box, click OK.
**Step 11** To trust the certificate, so you do not receive the dialog box again, click Yes.

**Tip** You can verify the certificate was installed successfully by clicking the Certification Path tab in the Certificate pane.

---

**What to Do Next**

You can copy the certificate to a file and store it locally so that you can restore the certificate whenever necessary.

**Related Topics**

- Copy web browser certificates to file, on page 12

---

**Copy web browser certificates to file**

You can copy certificates to local files and restore the certificates later whenever necessary.

Performing the following procedure copies the certificate using a standard certificate storage format for the following browsers:

- Internet Explorer 7
- Internet Explorer 8
- Safari 4.x

**Procedure**

**Step 1** View the certificate.

a) For Internet Explorer, click the Certificate Error status box, then click View Certificates.
b) For Safari 4.x, click **Show Certificate** in the Security Alert dialog box.

**Tip** In Safari, click the Certificate Error status box to display the Show Certificate option.

**Step 2** Click the **Details** tab.

**Step 3** Click the **Copy to File** button.

**Step 4** The Certificate Export Wizard displays. Click **Next**.

**Step 5** The following list defines the file formats from which you can choose. Choose the file format that you want to use for the exported file; click **Next**.

a) **DER encoded binary X.509 (.CER)**—Uses DER to transfer information between entities.

b) **Base-64 encoded X.509 (.CER)**—Sends secure binary attachments over the internet; uses ASCII text format to prevent corruption of file.

c) **Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)**—Exports the certificate and all certificates in the certification path to the chosen PC.

**Step 6** Browse to the location to which you want to export the file copy and name the file. Click **Save**.

**Step 7** The file name and path display in the **Certificate Export Wizard** pane. Click **Next**.

**Step 8** Your file and settings display. Click **Finish**.

**Step 9** When the successful export dialog box displays, click **OK**.

---

**Copy FireFox certificate to file**

You can copy the certificate to a local file and restore the certificate later whenever necessary.

Performing the following procedure copies the certificate by using a standard certificate storage format. To copy the certificate contents to file, perform the following procedure.

**Procedure**

**Step 1** From the FireFox browser, click **Tools > Options**. The Options dialog box displays.

**Step 2** If it is not already selected, click **Advanced**.

**Step 3** Click the Encryption tab and click **View Certificates**. The Certificate Manager dialog box displays.

**Step 4** Click the **Servers** tab.

**Step 5** Highlight the certificate you want to copy and click **Export**. The Save Certificate to File dialog box displays.

**Step 6** Browse to the location to which you want to copy the file.

**Step 7** From the Save as type drop-down list, choose the file type from the following options:

a) **X.509 Certificate (PEM)**—Uses PEM to transfer information between entities.

b) **X.509 Certificate with chain (PEM)**—Uses Privacy Enhanced Mail to verify the certificate chain and transfer information between entities.

• **X.509 Certificate (DER)**—Uses DER to transfer information between entities.
• X.509 Certificate (PKCS#7)—PKCS#7 is a standard for signing or encrypting data. Since the certificate is needed to verify signed data, it is possible to include it in the SignedData structure. A .P7C-file is just a degenerated SignedData structure, without any data to sign.

• X.509 Certificate with chain (PKCS#7)—Uses PKCS#7 to verify the certificate chain and transfer information between entities.

Step 8 Click Save.
Step 9 Click OK.

What to Do Next
You can copy the certificate to a file and store it locally so that you can restore the certificate whenever necessary.

Cisco Unified Communications Manager Administration application

You use Cisco Unified Communications Manager Administration, a web-based application, to perform configuration tasks for Cisco Unified Communications Manager servers. This section describes basic elements of the graphical user interface, including the navigation menus and the documentation search feature that allows you to search Cisco Unified Communications Manager documentation on Cisco.com.

Cisco Unified Communications Manager Administration Graphical User Interface

After you log in, the main Cisco Unified Communications Manager Administration window redisplays. The window includes the drop-down list box in the upper, right corner called Navigation. To access the applications in the drop-down list box, choose the program that you want and click Go.

Note
The minimum supported screen resolution specifies 1024x768. Devices with lower screen resolutions may not display the applications correctly.

Related Topics
   Introduction, on page 3
   Navigation drop-down list box, on page 14
   Links to Search documentation, About, and Logout, on page 15
   Menu bar, on page 15
   Shared login, on page 15

Navigation drop-down list box
The choices in the Navigation drop-down list box include the following Cisco Unified Communications Manager applications:
• Cisco Unified Communications Manager Administration—Shows as default when you access Cisco Unified Communications Manager. Use Cisco Unified Communications Manager Administration to configure system parameters, route plans, devices, and much more.

• Cisco Unified Serviceability—Takes you to the main Cisco Unified Serviceability window that is used to configure trace files and alarms and to activate and deactivate services.

• Cisco Unified OS Administration—Takes you to the main Cisco Unified OS Administration window, so you can configure and administer the Cisco Unified Communications Manager platform. You must log out from any other application before you can log in to this application.

• Disaster Recovery System—Takes you to the Cisco Disaster Recovery System, a program that provides full data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster. You must log out from any other application before you can log in to this application.

• Cisco Unified Reporting—Takes you to the main Cisco Unified Reporting window where you can generate system reports.

**Links to Search documentation, About, and Logout**

The following links display on the main Cisco Unified Communications Manager Administration window directly below the Navigation drop-down list box:

• Search Documentation—Click this link to search Cisco Unified Communications Manager documentation on Cisco.com for the current release. The Cisco Unified CM Documentation Search window displays. Type the word or words for which you want to search and click the Search button. The search results display. You can narrow the search results by choosing a documentation type modifier button that displays above your search result; for example, Unified CM Install/Upgrade or Unified CM Business Edition Release Notes.

• About—Click this link to display the Cisco Unified Communications Manager Administration main window where you can view the system software version.

• Logout—Click this link to log out of the Cisco Unified Communications Manager Administration application. The window redisplay with the login fields.

**Menu bar**

The horizontal bar located across the top of the interface contains the names of the menus. Click the menu options to display the Cisco Unified Communications Manager Administration windows. Menu items in this document appear in boldface font. A > (greater than) symbol separates menu item selections. In the browser, this indicates a menu item selection; for example: Choose Advanced Features > Intercompany Media Services > Service.

**Shared login**

After you log in to Cisco Unified Communications Manager Administration, you can access all applications that display in the Navigation drop-down list box, except the Cisco Unified Operating System Administration and Disaster Recovery System, without needing to log in to each application. You cannot access the Cisco Unified Operating System Administration or Disaster Recovery System GUIs with the same username and password that you use to access Cisco Unified Communications Manager Administration. To access these applications from Cisco Unified Communications Manager Administration, you must first click the Logout.
link in the upper, right corner of the Cisco Unified Communications Manager Administration window; then, choose the application from the Navigation drop-down list box and click Go.

If you have already logged in to one of the applications that display in the Navigation drop-down list box (other than Cisco Unified Operating System Administration or Disaster Recovery System), you can access Cisco Unified Communications Manager Administration without logging in. From the Navigation drop-down list box, choose Cisco Unified Communications Manager Administration and click Go.

**Cisco Unified Communications Manager Administration Help**

To access Help, click the Help menu in the Cisco Unified Communications Manager Administration navigation menu, and choose one of the following options:

- **Contents**—Opens a new browser window and displays the home page for the Cisco Unified Communications Manager Administration Help system. The links in the left pane of the Help window allow you to access all topics in the Help system.

- **This Page**—Opens a new browser window for the Cisco Unified Communications Manager Administration Help system. The right pane of the window contains definitions for each field in the current window in Cisco Unified Communications Manager Administration. In most cases, cross-references point to additional topics that relate to the current window.

- **About**—Displays the Cisco Unified Communications Manager Administration main window where you can view the system software version.

The left pane of the Help system provides a table of contents for all of the product guides that the Help system includes. The table of contents expands to show the location within the hierarchy of the Help topic that displays on the right.

To learn more about the Cisco Unified Communications Manager Administration system, including instructions on how to search Help, click the Using Help link at the top of any Help window.

**Find and delete records**

You can search Cisco Unified Communications Manager for any records that you have added to the database through the Cisco Unified Communications Manager Administration windows or for records that exist as default entries. To find records, you navigate to the Find and List window for the record that you want to locate, such as Find and List Phones (Device > Phone). You can search for all records or enter search criteria to narrow your search. The search parameters vary, depending on the records for which you are searching. For example, when searching for a phone, you can search for phones with certain digits in the directory number or certain characters in the device name. When searching for an end user, you can search for first names or last names that contain certain letters.

Once you have found records, you can delete them from the Find and List window that contains your records. You can delete individual records or delete all records that display in the window.

---

**Note**

During your work in a browser session, the cookies on the client machine store your find/list search preferences. If you navigate to other menu items and return to this menu item, or if you close the browser and then reopen a new browser window, your Cisco Unified Communications Manager search preferences get retained until you modify your search.
Use the following procedure to find or delete records from Cisco Unified Communications Manager Administration.

**Procedure**

**Step 1** Navigate to the Find and List window in Cisco Unified Communications Manager Administration for the component that you want to find. For example, if you want to find a phone, choose Device > Phone to display the Find and List Phones window.

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

**Step 3** To filter or search records
   a) From the first drop-down list box, select a search parameter. The search parameter represents the field on which you want to search. The search parameters vary, depending on the records type.
   b) From the second drop-down list box, select a search pattern. The search pattern defines how the system searches the records. For example, you might want to search for records (or search parameters) that contain a certain value that you specify in the search text field.
   c) Specify the appropriate search text, if applicable. The search text allows you to specify values for which you want to search. Use this field in conjunction with the search parameter and search pattern fields. For example, if you choose "Directory Number" from the search parameter drop-down list box, choose "contains" from the search pattern drop-down list box, and enter 5551212 as the search text, the system searches for a directory number that contains the digits 5551212.

**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.
You can reverse the sort order, by clicking the Up Arrow or Down Arrow, if available, in the list header.

**Note** You can delete multiple records from the database by checking the check boxes next to the appropriate record(s) and clicking **Delete Selected**. You can delete all configurable records for this selection by clicking the check box at the top of the column of check boxes 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.
The window displays the item that you choose.

**Related Topics**

- GUI buttons and icons, on page 18

**Add and copy records**

You can add items to the Cisco Unified Communications Manager by creating new records in Cisco Unified Communications Manager Administration and sometimes by copying existing records. Use the following procedure to add or copy records to the database.
Procedure

Step 1 Navigate to the Find and List window in Cisco Unified Communications Manager Administration for the component that you want to add or copy. For example, if you want to add a transcoder, choose Media Resources > Transcoder to display the Find and List Transcoders window.

Step 2 To add a new record, click the Add New button. The window refreshes with a new record. Make the necessary changes, and click Save.

Step 3 To copy an existing record, do one of the following:
   a) Use the Find and List window to display a set of records. From the list of records, click the Copy icon for a particular record, if the icon is available.
   b) Locate the record that you want to copy. Choose the record, which causes the complete record to display. Click the Copy icon in the configuration window. For example, find the transcoder that you want to copy, and click the Copy icon in the Transcoder Configuration window. The window refreshes with a new record. Make the necessary changes, and click Save.

   Note You must make a change to the copied record before you save the copy. If you do not, the system does not save the copy.

Step 4 To copy an existing record and populate a new record with all of the associated information from the existing record:
   a) Use the Find and List window to display a set of records. From the list of records, click the Super Copy icon for a particular record, if the icon is available.
   b) Locate the record that you want to copy. Choose the record, which causes the complete record to display. Click the Super Copy button in the configuration window. For example, find the phone record that you want to copy, and click the Super Copy button in the Phone Configuration window. The window refreshes with a new Device Name field. Make the necessary changes, and click Save.

Related Topics

Find and delete records, on page 16
GUI buttons and icons, on page 18

GUI buttons and icons

The Cisco Unified Communications Manager Administration windows use a common set of buttons and icons across the GUI. In general, icons display in a row that follows the window name, and a matching set of buttons displays near the bottom of the window.

Note Not all buttons and icons display on all windows. For those buttons that are not listed here, the individual configuration settings tables for each record type describe buttons that pertain to particular record types.

The Cisco Unified Communications Manager Administration GUI has the following groups of buttons and icons:

• Buttons and Icons on Find and List Windows
Buttons and Icons on Configuration Windows

Find and List Window buttons and icons

The following icons and buttons are found in the Find and List windows of the Cisco Unified Communications Manager Administration GUI:

- **Add New**—Opens a blank window of the same record type. Add configuration details to the new record and click Save, or choose an option in the Related Links drop-down list box.

- **Select All**—Chooses all of the records of a particular type that you are displaying. The check boxes to the left of each record get checked.

  **Note** This button selects only the records on the particular page that you are displaying.

  **Note** Example: Your search for partitions yielded 300 partitions, but you are only displaying 50 rows per page. If you click Select All while displaying any set of 50 partitions, only those 50 partitions get checked.

- **Clear All**—Deselects all of the records of a particular type that you are displaying. The check boxes to the left of each record get unchecked.

- **Delete Selected**—After you display a set of records, deletes the records for which you have checked the check boxes at left. You must confirm the deletion before the deletion takes place.

- **Reset Selected**—After you display a set of records, resets the records for which you have checked the check boxes at left. A popup window opens and offers the following choices:
  - **Reset**—Shuts down the device(s) and then restarts it (them).
  - **Restart**—Restarts the device(s) without shutting it (them) down.
  - **Close**—Closes the popup window without taking any action.

- **Apply Config to Selected**—When you change the configuration settings of a record, you may receive a message that directs you to click the Apply Config button to have the changes take effect. You can wait until you finish configuring multiple devices, then return to the Find and List window. Select the reconfigured devices and click the Apply Config to Selected button. A popup window advises of the possible actions that will take place when you click OK.

- **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.

- **Find**—Initiates a search for all records that match the criteria that you entered.

- **Clear Filter**—Removes all added search criteria from a search.

- **+(Plus button)**—To add additional search criteria to a search, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify.

- **–(Minus button)**—To remove criteria from a search, click the – button to remove the last added criterion.
• First-page Arrow—In a multipage list of records, click the First-page Arrow to display the first page of records.
• Left Arrow—In a multipage list of records, click the Left Arrow to display the preceding page of records.
• Right Arrow—In a multipage list of records, click the Right Arrow to display the following page of records.
• Last-page Arrow—In a multipage list of records, click the Last-page Arrow to display the last page of records.
• Go—In a multipage list of records, enter a value for the page of records to display; then, click Go.

**Configuration windows buttons and icons**

The following icons and buttons are found in the Configuration windows of the Cisco Unified Communications Manager Administration GUI:

• Save—Saves the current record.
• Delete—Deletes the current record after requesting confirmation of the deletion.
• Copy—Refreshes the window with a copy of the current record. You must change at least one value (usually, the record name) before you can save the copied record by clicking **Save**.
• Reset—Opens a popup window that offers the following choices:
  ◦ Reset—Shuts down the device and then restarts it.
  ◦ Restart—Restarts the device without shutting it down.
  ◦ Close—Closes the popup window without taking any action.
• Apply Config—When you change the configuration settings of a record, you may receive a message that directs you to click the **Apply Config** button to have the changes take effect. When you click the **Apply Config** button, a popup window advises of the possible actions that will take place when you click **OK**.
• Add New—Opens a blank window of the same record type. Add configuration details to the new record and click **Save**, or choose an option in the Related Links drop-down list box.
• Next—For record types that require multiple steps to add a new record, the Next button takes you from one step to the next.

**Cisco Unified Presence server access**

If you have configured a Cisco Unified Presence server, the Cisco Unified Communications Manager Administration main window provides a link directly to the associated Cisco Unified Presence server. To access Cisco Unified Presence Administration, click the Cisco Unified Presence address link.
**Clustered Cisco Unified Presence server access**

If you have a Cisco Unified Presence server configured as part of the Cisco Unified Communications Manager cluster, the main Cisco Unified Communications Manager Administration window displays a link to the Cisco Unified Presence publisher server.

To access Cisco Unified Presence Administration, click the link to the Cisco Unified Presence publisher server.

**Login message customization**

You can upload a text file that contains a customized login message that displays in the main Cisco Unified Communications Manager Administration window.

For more information and the procedure for uploading your customized login message, see the *Cisco Unified Communications Operating System Administration Guide*.

**Last successful login message**

When you log in to Cisco Unified Communications Manager Administration, the main Cisco Unified Communications Manager Administration window displays the date and time of the last successful system login.

When you log in to Cisco Unified Communications Manager for the first time, the system displays the last successful login time as the current time.

**Accessibility**

Cisco Unified Communications Manager Administration and Cisco Unified CM User Options provide functionality for users that allows them to access buttons on the window without using a mouse. You can perform the following procedures from any point on the window, so the user does not have to scroll or tab through various fields.

**Access icons**

Many of the windows in Cisco Unified Communications Manager include icons that display at the top of the window; for example, an icon of a disk for Save, an icon that is a plus sign (+) for Add, and so on. To access these icons, perform the following procedure.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Press Alt, press 1; then, press Tab. The cursor will highlight the first icon from the left. To move to the next icon, press Tab again.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Press Enter. The system performs the function of the icon; for example, Add.</td>
</tr>
</tbody>
</table>
Access buttons

Many of the windows in Cisco Unified Communications Manager and Cisco PCA have buttons that display at the bottom of the window; for example, a button for Save, a button for Add, and so on. To access these buttons, perform the following procedure.

Procedure

Step 1 Press Alt, press 2, and then press Tab. The cursor will highlight the first button from the left. To move to the next button, press Tab again.

Step 2 Press Enter. The function of the button gets performed; for example, Save.

Where to find more information

- Cisco Unified Communications Manager System Guide
- Cisco Unified Communications Manager Features and Services Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide
- Installing Cisco Unified Communications Manager
- Upgrading Cisco Unified Communications Manager
- Cisco Unified Communications Manager Security Guide
- Cisco Unified Communications Operating System Administration Guide
- Disaster Recovery System Administration Guide
- Cisco Unified Communications Solution Reference Network Design (SRND)
PART II

System setup

- Server setup, page 25
- Cisco Unified Communications Manager setup, page 33
- Cisco Unified Communications Manager group setup, page 39
- Phone NTP reference setup, page 43
- Date and time group setup, page 47
- Region setup, page 53
- Device pool setup, page 63
- DHCP server setup, page 81
- DHCP subnet setup, page 85
- LDAP system setup, page 89
- LDAP directory setup, page 93
- LDAP authentication setup, page 101
- LDAP custom filter setup, page 105
- Location setup, page 107
- Survivable remote site telephony setup, page 115
- MLPP Domain setup, page 119
- Resource Priority Namespace Network Domain setup, page 121
• Resource Priority Namespace List setup, page 123
• E911 messages, page 125
• Enterprise parameter setup, page 127
• Enterprise phone setup, page 129
• Service parameter setup, page 131
• Application server setup, page 135
• Autoregistration setup, page 139
• Other system menu options, page 145
Server setup

This chapter provides information about server configuration.

See also Internet Protocol Version 6 (IPv6) in Cisco Unified Communications Manager Features and Services Guide and Changing the IP Address and Host Name for Cisco Unified Communications Manager.

- About server setup, page 25
- Server deletion, page 26
- Add node to cluster before install, page 27
- Add deleted server back in to cluster, page 28
- Server settings, page 29
- View Presence Server Status, page 31

About server setup

In Cisco Unified Communications Manager Administration, use the System > Server menu path to add and configure a server.

Use the Server Configuration window to specify the address of the server where Cisco Unified Communications Manager or Cisco Unified Communications Manager IM and Presence Service is installed.

Server setup tips

Before you configure a server, review the following information:

- Make sure that you only add each server once in the Server Configuration window. If you add a server by using the hostname and add the same server again by using the IP address, Cisco Unified Communications Manager cannot accurately determine component versions for the server after a Cisco Unified Communications Manager upgrade. If you have two entries in Cisco Unified Communications Manager Administration for the same server, delete one of the entries before you upgrade.

- When you perform a fresh installation of Cisco Unified Communications Manager, you must define any subsequent servers (nodes) in the Server Configuration window using Cisco Unified Communications Manager Administration before you can install Cisco Unified Communications Manager or IM and Presence Service on each subsequent server. To define a subsequent node, click Add New and proceed
to configure the server. After you add the subsequent server, you can then install the Cisco Unified Communications Manager or IM and Presence Service software on that server.

- If you use IPv4 in your network, you must update the DNS server with the appropriate Cisco Unified Communications Manager name and address information before you use that information to configure the Cisco Unified Communications Manager server.

Caution

If your network supports IPv6 or IPv4 and IPv6 in dual-stack mode, 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.

- For DNS, make sure that you map the IP addresses of all servers, including dummy nodes, to the host names on the DNS server. If you do not perform this task, Cisco Unified Communications Manager generates alarms that inform you that the License Manager service is down.

- Cisco Unified Communications Manager Administration does not prevent you from updating the Host Name/IP Address field under any circumstances.

- When you attempt to change the IP address in the Server Configuration window, the following message displays after you save the configuration: "Changing the host name/IP Address of the server may cause problems with Cisco Unified Communications Manager. Are you sure that you want to continue?" Before you click OK, make sure that you understand the implications of updating the Host Name/IP Address field; for example, incorrectly updating this setting may cause Cisco Unified Communications Manager to become inoperable; that is, the database may not work, you may not be able to access Cisco Unified Communications Manager Administration, and so on. In addition, updating this field without performing other related tasks may cause problems for Cisco Unified Communications Manager.

- Changes to the server configuration do not take effect until you restart Cisco Unified Communications Manager. For information about restarting the Cisco CallManager service, see the Cisco Unified Serviceability Administration Guide.

- For additional information on changing the IP address or host name, see the document Changing the IP Address and Host Name for Cisco Unified Communications Manager.

Related Topics

Server deletion, on page 26

Server deletion

This section describes how to delete a server from the Cisco Unified Communications Manager database and how to add a deleted server back to the Cisco Unified Communications Manager cluster.

In Cisco Unified Communications Manager Administration, you cannot delete the first node of the cluster, but you can delete subsequent nodes. Before you delete a subsequent node in the Find and List Servers window, Cisco Unified CM Administration displays the following message: “You are about to permanently delete one or more servers. This action cannot be undone. Continue?”. If you click OK, the server gets deleted from the Cisco Unified CM database and is not available for use.
When you attempt to delete a server from the Server Configuration window, a message that is similar to the one in the preceding paragraph displays. If you click OK, the server gets deleted from the Cisco Unified CM database and is not available for use.

Before you delete a server, consider the following information:

- Cisco Unified Communications Manager Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node.

- Cisco recommends that you do not delete any node that has Cisco Unified Communications Manager running on it, especially if the node has devices, such as phones, registered with it.

- Although dependency records exist for the subsequent nodes, the records do not prevent you from deleting the node.

- If any call park numbers are configured for Cisco Unified Communications Manager on the node that is being deleted, the deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified Communications Manager Administration.

- If a configuration field in Cisco Unified Communications Manager Administration contains the IP address or host name for a server that you plan to delete, update the configuration before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server; for example, if you enter the IP address or host name for a service parameter, enterprise parameter, service URL, directory URL, IP phone service, and so on, update this configuration before you delete the server.

- If an application GUI, for example, Cisco Unity, Cisco Unity Connection, and so on, contains the IP address or host name for the server that you plan to delete, update the configuration in the corresponding GUIs before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server.

- The system may automatically delete some devices, such as MOH servers, when you delete a server.

- Before you delete a node, Cisco recommends that you deactivate the services that are active on the subsequent node. Performing this task ensures that the services work after you delete the node.

- Changes to the server configuration do not take effect until you restart Cisco Unified Communications Manager. For information on restarting the Cisco CallManager service, see the Cisco Unified Serviceability Administration Guide.

- To ensure that database files get updated correctly, you must reboot the cluster after you delete a server, Presence, or application server.

- After you delete the node, access Cisco Unified Reporting to verify that Cisco Unified Communications Manager removed the node from the cluster. In addition, access Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes by using the CLI.

Add node to cluster before install

Use Cisco Unified Communications Manager Administration to add a new node to a cluster before installing the node. The server type you select when adding the node must match the server type you install.
You must configure a new node on the first node using Cisco Unified Communications Manager Administration before you install the new node. To install a node on a cluster, see the *Cisco Unified Communications Manager Installation Guide*.

For Cisco Unified Communications Manager Video/Voice servers, the first server you add during an initial installation of the Cisco Unified Communications Manager software is designated the publisher node. All subsequent server installations or additions are designated as subscriber nodes. The first Cisco Unified Communications Manager IM and Presence node you add to the cluster is designated the IM and Presence Service database publisher node.

**Note**

You cannot use Cisco Unified Communications Manager Administration to change the server type after the server has been added. You must delete the existing server instance, and then add the new server again and choose the correct server type setting.

---

**Procedure**

**Step 1**
Select **System > Server**. The *Find and List Servers* window displays.

**Step 2**
Click **Add New**. The *Server Configuration - Add a Server* window displays.

**Step 3**
From the **Server Type** drop-down list box, choose the server type that you want to add, and then click **Next**.
- CUCM Video/Voice
- CUCM IM and Presence

**Step 4**
In the **Server Configuration** window, enter the appropriate server settings. For server configuration field descriptions, see topics related to server settings.

**Step 5**
Click **Save**.

**Related Topics**

- Server settings, on page 29

---

**Add deleted server back in to cluster**

If you delete a subsequent node (subscriber) from Cisco Unified Communications Manager Administration and you want to add it back to the cluster, perform the following procedure.

**Procedure**

**Step 1**
In Cisco Unified Communications Manager Administration, add the server by choosing **System > Server**.

**Step 2**
After you add the subsequent node to Cisco Unified Communications Manager Administration, perform an installation on the server by using the disk that Cisco provided in your software kit.
For example, if you have a version 8.5(1) disk, perform a 8.5(1) installation on the node. If you have a disk with a compatible version of 6.1(3) on it, for example, use the disk to install Cisco Unified CM on the subsequent node; during the installation, choose the Upgrade During Install option when the installation displays the options.

Make sure that the version that you install on the subsequent node matches the version that runs on the first node (publisher) in the cluster.

If the first node in the cluster runs Cisco Unified Communications Manager 8.5(1) version and a service update (or engineering special), you must choose the Upgrade During Install option when the installation displays the installation options; before you choose this option, ensure that you can access the service update (or engineering special) image on DVD or a remote server. For more information on how to perform an installation, see the installation documentation that supports your version of Cisco Unified Communications Manager.

Step 3 After you install Cisco Unified CM, configure the subsequent node, as described in the installation documentation that supports your version of Cisco Unified CM.

Step 4 Access the Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

Server settings

The following table describes the Cisco Unified Communications Manager voice/video server configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Information</td>
<td></td>
</tr>
<tr>
<td>Host Name/IP Address</td>
<td>If your network uses DNS that can map to IPv4 addresses, you can enter the</td>
</tr>
<tr>
<td></td>
<td>host name of the Cisco Unified Communications Manager server. Otherwise,</td>
</tr>
<tr>
<td></td>
<td>you must enter the full IPv4 address of the server.</td>
</tr>
<tr>
<td>Tip</td>
<td>To avoid errors, Cisco recommends that you add a server to the system with</td>
</tr>
<tr>
<td></td>
<td>a name that has less than 47 characters. Then, update the server name to</td>
</tr>
<tr>
<td></td>
<td>the target length.</td>
</tr>
<tr>
<td>Tip</td>
<td>If your network supports IPv6 (or IPv4 and IPv6), configure the IPv6 Name</td>
</tr>
<tr>
<td></td>
<td>field in addition to the Hostname/IP Address field.</td>
</tr>
<tr>
<td>Note</td>
<td>You must update the DNS server with the appropriate Cisco Unified</td>
</tr>
<tr>
<td></td>
<td>Communications Manager name and address information before you enter that</td>
</tr>
<tr>
<td></td>
<td>information in this field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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 <em>Cisco Unified Communications Manager Features and Services Guide</em>. This field, which gets included in the TFTP configuration file, gets used by phones that run SCCP to retrieve the IPv6 address of the Cisco Unified Communications Manager server, so phone registration occurs. <strong>Tip</strong> Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information. <strong>Caution</strong> If your network supports IPv6 or IPv4 and IPv6 in dual-stack mode, 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 IP Address/Hostname field, so Cisco Unified Communications Manager can support features/devices that use IPv4 (or IPv4 and IPv6).</td>
</tr>
<tr>
<td>MAC Address</td>
<td>This field is optional. It exists only to give you a place to note the server MAC address. It does not impact the system at all. Enter the media access control (MAC) address of the network interface card (NIC) in the Cisco Unified Communications Manager server. The MAC address specifies the permanent hardware address of the NIC. <strong>Tip</strong> If you plan to move the server periodically to different locations on the network, you must enter the MAC address, so other devices on the network can always identify the server. If you do not plan to relocate the server, consider entry of the MAC address as optional.</td>
</tr>
<tr>
<td>Description</td>
<td>Consider this entry as optional. Enter a description of the server. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Location Bandwidth Management Information</td>
<td></td>
</tr>
<tr>
<td>LBM Intercluster Replication Group</td>
<td>Select an LBM Intercluster Replication Group from the drop-down list. You may also click <strong>View Details</strong> to display the settings for this LBM Intercluster Replication Group.</td>
</tr>
</tbody>
</table>
Related Topics

Server setup, on page 25

View Presence Server Status

Use Cisco Unified Communications Manager Administration to view the status of critical services and self-diagnostic test results for the IM and Presence Service node.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select System &gt; Server. The <strong>Find and List Servers</strong> window appears.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select the server search parameters, and then click <strong>Find</strong>. Matching records appear.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select the IM and Presence server that is listed in the <strong>Find and List Servers</strong> window. The <strong>Server Configuration</strong> window appears.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click on the Presence Server Status link in the IM and Presence Server Information section of the <strong>Server Configuration</strong> window. The <strong>Node Details</strong> window for the server appears.</td>
</tr>
</tbody>
</table>


View Presence Server Status
Cisco Unified Communications Manager setup

This chapter provides information to find and update a Cisco Unified Communications Manager configuration or to view system component version information.

See also Cisco Unified Serviceability Administration Guide.

- About Cisco Unified Communications Manager setup, page 33
- Cisco Unified Communications Manager settings, page 33
- Synchronize Cisco Unified Communications Manager with devices, page 37
- Activate Cisco CallManager service, page 37
- Deactivate Cisco CallManager service, page 38

About Cisco Unified Communications Manager setup

In Cisco Unified Communications Manager Administration, use the System > Cisco Unified CM menu path to configure Cisco Unified Communications Managers.

Use Cisco Unified Communications Manager configuration to specify the ports and other properties for the Cisco Unified Communications Manager.

Note: In Cisco Business Edition 5000 systems, only one Cisco Unified Communications Manager exists.

Cisco Unified Communications Manager settings

The following table describes the Cisco Unified Communications Manager settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Information</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CTI ID</td>
<td>This read-only field displays the computer telephony integration (CTI) identification.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Server</td>
<td>This read-only field displays the server where this Cisco Unified Communications Manager is installed.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Name</td>
<td>Enter the name that you want to assign to this Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the Cisco Unified Communications Manager. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Location Bandwidth Manager Group</td>
<td>Select a Location Bandwidth Manager Group from the drop-down list.</td>
</tr>
</tbody>
</table>

**Auto-registration Information**

You must configure the Universal Device Template and Universal Line template before you configure auto-registration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Directory Number</td>
<td>Enter the first directory number to use for autoregistration of devices. Do not begin the Starting Directory Number with a zero (0).</td>
</tr>
</tbody>
</table>
| Ending Directory Number                        | Enter the last directory number to use for autoregistration of devices. Do not begin the Ending Directory Number with a zero (0).  
Note: The Ending Directory Number must be greater than the Starting Directory Number which automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.  
Tip: You must choose a range for autoregistration before you can choose a partition, external phone number mask or voice messaging box mask. If more than 250 partitions exist, the Find button displays next to the drop-down list box. |
| Partition                                      | If you are not using partitions, choose <None>. If you are using partitions, choose the partition to which autoregistered directory numbers belong from the drop-down list box.  
Tip: You must choose a range for autoregistration before you can choose a partition, external phone number mask or voice messaging box mask. If more than 250 partitions exist, the Find button displays next to the drop-down list box. |

1. To display the Find and List Partitions window, click the Find button.
2. In the List items where Name contains field, enter a partial partition name.
3. In the list of partitions that displays in the Select item to use box, click the desired partition name.
4. Click OK.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Phone Number Mask</td>
<td>Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the autoregistered devices.</td>
</tr>
<tr>
<td></td>
<td>• The mask can contain up to 50 characters.</td>
</tr>
<tr>
<td></td>
<td>• Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the autoregistered device.</td>
</tr>
<tr>
<td></td>
<td>See the following examples:</td>
</tr>
<tr>
<td></td>
<td>• If you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234 if the Use External Phone Number Mask option is checked on the route pattern that is used to make the external call.</td>
</tr>
<tr>
<td></td>
<td>• If you specify a mask of all literal digits, such as 9728135000 to represent a main attendant number, that literal number (9728135000) displays as the caller ID for an external call from any autoregistered device.</td>
</tr>
<tr>
<td></td>
<td>Auto-registration Disabled on this Cisco Unified Communications Manager</td>
</tr>
<tr>
<td></td>
<td>• To enable autoregistration for this Cisco Unified Communications Manager, uncheck the Auto-registration Disabled check box.</td>
</tr>
<tr>
<td></td>
<td>• To disable autoregistration for this Cisco Unified Communications Manager, check the Auto-registration Disabled check box.</td>
</tr>
<tr>
<td></td>
<td>• When autoregistration is disabled, you must configure the directory numbers manually whenever you add new devices to your network.</td>
</tr>
<tr>
<td></td>
<td>• Setting the Starting Directory Number and Ending Directory Number to the same value also disables autoregistration.</td>
</tr>
<tr>
<td></td>
<td>• If starting and ending directory numbers are currently specified when you disable autoregistration by checking this option, Cisco Unified Communications Manager sets the starting and ending directory numbers to the same value.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager resets the partition and external phone mask information when autoregistration is disabled.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ethernet Phone Port</td>
<td>Cisco Unified Communications Manager uses this TCP port to communicate with the Cisco Unified IP Phones (SCCP only) on the network.</td>
</tr>
<tr>
<td></td>
<td>• Accept the default port value of 2000 unless this port is already in use on your system. Choosing 2000 identifies this port as non-secure.</td>
</tr>
<tr>
<td></td>
<td>• Ensure all port entries are unique.</td>
</tr>
<tr>
<td></td>
<td>• Valid port numbers range from 1024 to 49151.</td>
</tr>
<tr>
<td></td>
<td>• See the <em>Cisco Unified Communications Manager Security Guide</em> for information about security configurations.</td>
</tr>
<tr>
<td>MGCP Listen Port</td>
<td>Cisco Unified Communications Manager uses this TCP port to detect messages from its associated MGCP gateway.</td>
</tr>
<tr>
<td></td>
<td>• Accept the default port of 2427 unless this port is already in use on your system.</td>
</tr>
<tr>
<td></td>
<td>• Ensure all port entries are unique.</td>
</tr>
<tr>
<td></td>
<td>• Valid port numbers range from 1024 to 49151.</td>
</tr>
<tr>
<td>MGCP Keep-alive Port</td>
<td>Cisco Unified Communications Manager uses this TCP port to exchange keepalive messages with its associated MGCP gateway.</td>
</tr>
<tr>
<td></td>
<td>• Accept the default port of 2428 unless this port is already in use on your system.</td>
</tr>
<tr>
<td></td>
<td>• Ensure all port entries are unique.</td>
</tr>
<tr>
<td></td>
<td>• Valid port numbers range from 1024 to 49151.</td>
</tr>
<tr>
<td>SIP Phone Port</td>
<td>This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations over TCP and UDP.</td>
</tr>
<tr>
<td>SIP Phone Secure Port</td>
<td>This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations over TLS.</td>
</tr>
<tr>
<td></td>
<td>See the <em>Cisco Unified Communications Manager Security Guide</em> for information about security configurations.</td>
</tr>
<tr>
<td>Reset button</td>
<td>Click this button to reset all devices that belong to the same Cisco Unified CM Group as this Cisco Unified Communications Manager server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> All devices in the Cisco Unified CM Group of which this server is a member get reset, not just those devices that are registered with this server.</td>
</tr>
</tbody>
</table>

**Related Topics**

*Cisco Unified Communications Manager setup, on page 33*
Synchronize Cisco Unified Communications Manager with devices

To synchronize a Cisco Unified Communications Manager that has undergone configuration changes with its corresponding registered devices, perform the following procedure, which applies 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 System > Cisco Unified CM.  
The Find and List Cisco Unified CMs window displays.

Step 2  Choose the search criteria to use.

Step 3  Click Find.  
The window displays a list of Cisco Unified CMs that match the search criteria.

Step 4  Click the Cisco Unified Communications Manager that you want to synchronize with its devices.

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.

Related Topics
Cisco Unified Communications Manager setup, on page 33

Activate Cisco CallManager service

When you perform a new Cisco Unified Communications Manager installation, you must follow these steps in sequence:

1  Add the server. Cisco Unified Communications Managers automatically get added when a server gets configured.

2  Activate the Cisco CallManager service, as described in the Cisco Unified Serviceability Administration Guide.

A message displays if you do not follow this sequence.

Related Topics
Cisco Unified Communications Manager setup, on page 33
Deactivate Cisco CallManager service

You can deactivate the Cisco CallManager service in Cisco Unified Serviceability. When you deactivate the Cisco CallManager service, the Cisco Unified Communications Manager where you deactivated the service becomes inactive for use.

---

**Note**

From Cisco Unified Serviceability, you can view the status of the Cisco Unified Communications Manager by accessing **Tools > Service Activation**.

---

**Note**

When the Cisco CallManager service is deactivated, no one can make calls on that Cisco Unified Communications Manager.

You may still be able to perform configuration operations on a deactivated Cisco Unified Communications Manager if the Cisco Communications Manager Administration web service is active and the database is up and running.

When you reactivate the Cisco CallManager service on the Cisco Unified Communications Manager, the database automatically re-creates the Cisco Unified Communications Manager by retaining the original configuration (server name or IP address). This Cisco Unified Communications Manager then becomes active; you can verify that the Cisco CallManager service is running by accessing **Tools > Control Center - Feature Services** in Cisco Unified Serviceability.

For more information about Service Activation, see the Cisco Unified Serviceability Administration Guide.

**Related Topics**

- Cisco Unified Communications Manager setup, on page 33
Cisco Unified Communications Manager group setup

This chapter provides information to configure a Cisco Unified Communications Manager group.

- About Cisco Unified Communications Manager group setup, page 39
- Cisco Unified Communications Manager group deletion, page 40
- Cisco Unified Communications Manager group settings, page 40
- Synchronize Cisco Unified Communications Manager Group settings with devices, page 42

About Cisco Unified Communications Manager group setup

In Cisco Unified Communications Manager Administration, use the System > Cisco Unified CM Group menu path to configure Cisco Unified Communications Manager groups.

A Cisco Unified Communications Manager Group specifies a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager for that group, and the other members of the group serve as secondary and tertiary (backup) Cisco Unified Communications Managers.

Each device pool has one Cisco Unified Communications Manager Group that is assigned to it. When a device registers, it attempts to connect to the primary (first) Cisco Unified Communications Manager in the group that is assigned to its device pool. If the primary Cisco Unified Communications Manager is not available, the device tries to connect to the next Cisco Unified Communications Manager that is listed in the group, and so on.

Cisco Unified Communications Manager Groups provide important features for your system:

- Redundancy—This feature enables you to designate a primary and backup Cisco Unified Communications Managers for each group.

- Call processing load balancing—This feature enables you to distribute the control of devices across multiple Cisco Unified Communications Managers.

For most systems, you need to have multiple groups, and you need to assign a single Cisco Unified Communications Manager to multiple groups to achieve better load distribution and redundancy.
Cisco Unified Communications Manager group configuration considerations

Before configuring a Cisco Unified Communications Manager group, you must configure the Cisco Unified Communications Managers that you want to assign as members of that group.

After you have configured the Cisco Unified Communications Manager group, you can use it to configure device pools. Devices obtain their Cisco Unified Communications Manager Group list setting from the device pool to which they are assigned.

Related Topics

About Cisco Unified Communications Manager setup, on page 33

Cisco Unified Communications Manager group deletion

You cannot delete a Cisco Unified Communications Manager group if it is assigned to any device pools or MGCP gateways or if it is the current Auto-registration Cisco Unified Communications Manager Group for the cluster.

To find out which devices are using the Cisco Unified Communications Manager group, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified Communications Manager Group Configuration window and click Go.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a Cisco Unified Communications Manager group that is in use, a message displays. Before deleting a Cisco Unified Communications Manager group that is currently in use, you must perform some or all of the following tasks:

• Assign a different Cisco Unified Communications Manager group to the device pools or MGCP gateways that currently use this Cisco Unified Communications Manager group.

• Create or choose a different Cisco Unified Communications Manager group to be the Auto-registration Cisco Unified Communications Manager Group.

Related Topics

About device pool setup, on page 63
Access dependency records, on page 874

Cisco Unified Communications Manager group settings

The following table describes the settings for Cisco Unified Communications Manager groups.

Table 3: Cisco Unified Communications Manager group settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager Group Settings</td>
<td></td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the new group.</td>
</tr>
<tr>
<td>Auto-registration Cisco Unified Communications Manager Group</td>
<td>Check the Auto-registration Cisco Unified Communications Manager Group check box if you want this Cisco Unified Communications Manager group to be the default Cisco Unified Communications Manager group when auto-registration is enabled. Leave this check box unchecked if you do not want devices to auto-register with this Cisco Unified Communications Manager group.</td>
</tr>
<tr>
<td>Tip</td>
<td>Each Cisco Unified Communications Manager cluster can have only one default auto-registration group. If you choose a different Cisco Unified Communications Manager group as the default auto-registration group, that is, you check the Auto-registration Cisco Unified Communications Manager Group check box for a different Cisco Unified Communications Manager group, the previously chosen auto-registration group no longer serves as the default for the cluster; the Auto-registration Cisco Unified Communications Manager check box displays for the previously chosen group (the original default), and the check box gets disabled for the group that now serves as the default.</td>
</tr>
</tbody>
</table>

---

### Cisco Unified Communications Manager Group Members

<table>
<thead>
<tr>
<th>Available Cisco Unified Communications Managers</th>
<th>This field displays the list of available Cisco Unified Communications Manager that are not a part of the Cisco Unified Communications Manager group. Choose the Cisco Unified Communications Manager names and use the up and down arrows to move Cisco Unified Communications Managers between the Selected list and the Available list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Cisco Unified Communications Managers</td>
<td>This field displays the Cisco Unified Communications Managers that are in the Cisco Unified Communications Manager group. The Selected list, which can contain up to three Cisco Unified Communications Managers, lists the Cisco Unified Communications Managers in order by highest priority. Cisco Unified Communications Managers in the Selected list become members of the group when you click <strong>Save</strong>. Choose the Cisco Unified Communications Manager names and use the up and down arrows to move Cisco Unified Communications Managers between the Selected list and the Available list. Within the Selected list, use the up and down arrows to arrange the groups in the Selected list in the order that you want.</td>
</tr>
</tbody>
</table>
Synchronize Cisco Unified Communications Manager Group settings with devices

To synchronize a Cisco Unified Communications Manager Group that has undergone recent configuration changes to their associated registered devices, perform the following procedure, which applies any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset or restart may not be required on some affected devices.)

Procedure

Step 1  Choose Media Resources > Cisco Unified CM Group. 
The Find and List Cisco Unified CM Groups window displays.

Step 2  Choose the search criteria to use.

Step 3  Click Find. 
The window displays a list of Cisco Unified CM Groups that match the search criteria.

Step 4  Click the Cisco Unified CM Group that you want to synchronize with affected devices. The Cisco Unified CM Group 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.
Phone NTP reference setup

This chapter provides information to configure phone NTP references.

- About phone NTP reference setup, page 43
- Phone NTP reference deletion, page 44
- Phone NTP reference settings, page 44

About phone NTP reference setup

In Cisco Unified Communications Manager Administration, use the System > Phone NTP Reference menu path to configure phone NTP references.

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

After you add the phone NTP reference to Cisco Unified Communications Manager Administration, you must add it to a date/time group. In the date/time group, you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

The date/time group configuration gets specified in the device pool, and the device pool gets specified on the phone page.

Phone NTP references setup tips

After you add a new phone NTP reference to the Cisco Unified Communications Manager database, assign it to a date/time group.

Related Topics

- About date and time group setup, on page 47
Phone NTP reference deletion

Before you can delete the phone NTP reference from Cisco Unified Communications Manager Administration, you must delete the phone NTP reference from the date/time group. To find which date/time groups use the phone NTP reference, choose Dependency Records from the Related Links drop-down list box in the Phone NTP Reference Configuration window and click Go. When you know which date/time groups use the phone NTP reference, you can then remove that phone NTP reference from that group.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

Related Topics

Access dependency records, on page 874

Phone NTP reference settings

The following table describes the phone NTP reference settings.

Table 4: Phone NTP reference settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP Address| Enter the IP address of the NTP server that you want the phone that is running SIP to use to get its date and time.  
**Note** Cisco Unified Communications Manager cannot be configured as Phone NTP References. |
| Description| Enter a description for the phone NTP reference. Cisco Unified Communications Manager Administration automatically propagates the information in the IP Address field to the Description field. If you want to do so, you can change the information. |
From the drop-down list box, choose the mode for the phone NTP reference. The values from which you can choose follow:

- **Directed Broadcast**—If you choose this default NTP mode, the phone accesses date/time information from any NTP server but gives the listed NTP servers (1st = primary, 2nd = secondary) priority. For example, if the phone configuration contains NTP servers where A = primary NTP server and B = secondary/backup NTP server, the phone uses the broadcast packets (derives the date/time) from NTP server A. If NTP server A is not broadcasting, the phone accesses date/time information from NTP server B. If neither NTP server is broadcasting, the phone accesses date/time information from any other NTP server. If no other NTP server is broadcasting, the phone will derive the date/time from the Cisco Unified Communications Manager 200 OK response to the REGISTER message.

- **Unicast**—If you choose this mode, the phone will send an NTP query packet to that particular NTP server. If the phone gets no response, the phone will access date/time information from any other NTP server. If no other NTP servers respond, the phone will derive the date/time from the Cisco Unified Communications Manager 200 OK response to the REGISTER message.

---

**Note**

Cisco Unified Communications Manager currently does not support the Multicast and Anycast modes. If you choose either of these modes, Cisco Unified Communications Manager will default to the Directed Broadcast mode.

---

**Related Topics**

Phone NTP reference setup, on page 43
Phone NTP reference settings
Date and time group setup

This chapter provides information to add, update, or delete Date/Time Groups, and to synchronize configuration changes with affected devices.

- About date and time group setup, page 47
- Add phone NTP reference to SIP phones in date and time group, page 48
- Date and time group deletion, page 49
- Date and time group settings, page 49
- Synchronize date and time group settings with devices, page 50

About date and time group setup

In Cisco Unified Communications Manager Administration, use the System > Date/Time Group menu path to configure date and time groups.

Use Date/Time Groups to define time zones for the various devices that are connected to Cisco Unified Communications Manager. Each device exists as a member of only one device pool, and each device pool has only one assigned Date/Time Group.

Installing Cisco Unified Communications Manager automatically configures a default Date/Time Group that is called CMLocal. CMLocal synchronizes to the active date and time of the operating system on the server where Cisco Unified Communications Manager is installed. After installing Cisco Unified Communications Manager, you can change the settings for CMLocal as desired. Normally, adjust server date/time to the local time zone date and time.

Note

CMLocal resets to the operating system date and time whenever you restart Cisco Unified Communications Manager or upgrade the Cisco Unified Communications Manager software to a new release. Do not change the name of CMLocal.

Tip

For a worldwide distribution of Cisco Unified IP Phones, create one named Date/Time Group for each of the time zones in which you will deploy endpoints.
Add phone NTP reference to SIP phones in date and time group

Use the following procedure to add a phone NTP reference to a date/time group for a phone that is running SIP.

**Procedure**

**Step 1** To add a phone NTP reference to a date/time group for a phone that is running SIP, perform the following tasks:

*Note* To get its date and time, a phone that is running SIP can use NTP server(s) that exist in Cisco Unified Communications Manager Administration.

a) Click the **Add Phone NTP References** button.

b) Find the phone NTP reference(s) that you want to add.

Only phone NTP references that exist in the Cisco Unified Communications Manager database display.

c) After the search results display, check the check boxes for any phone NTP references that you want to add to the date/time group or click **Select All**.

d) Click **Add Selected**.

Tip After you add the phone NTP reference(s) to the date/time group, you can prioritize them, starting with the first server that you want the phone that is running SIP to contact. For example, to move a server to the top of the list, highlight the entry in the pane and click the Up arrow. To move a server to the bottom of the list, highlight the entry in the pane and click the Down arrow.

**Step 2** To remove a phone NTP reference from the date/time group, highlight the reference in the pane and click **Remove Phone NTP References**.

Removing the phone NTP reference from the date/time group does not remove the phone NTP reference from the Cisco Unified Communications Manager database.

**Step 3** To save the new date/time group in the database, click the **Save** icon that displays in the tool bar in the upper, left corner of the window (or click the **Save** button that displays at the bottom of the window).

*Note* See the procedure to synchronize a Date/Time group with affected devices before deciding on whether to proceed to the next step.

**Step 4** To reset the devices that use the date/time group, click **Reset**.

**What to Do Next**

After adding a new date/time group to the database, you can assign it to a device pool to configure the date and time information for that device pool.

**Related Topics**

- Phone NTP reference setup, on page 43
- About phone NTP reference setup, on page 43
- Synchronize date and time group settings with devices, on page 50
- About device pool setup, on page 63
### Date and time group deletion

**Note**
You cannot delete a date/time group that any device pool uses.

To find out which device pools use the date/time group, choose **Dependency Records** from the Related Links drop-down list box on the Date/Time Group Configuration window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a date/time group that is in use, Cisco Unified Communications Manager displays a message. Before deleting a date/time group that is currently in use, you must perform either or both of the following tasks:

- Assign a different date/time group to any device pools that use the date/time group that you want to delete.
- Delete the device pools that use the date/time group that you want to delete.

**Related Topics**
- About device pool setup, on page 63
- Device pool deletion, on page 64
- Access dependency records, on page 874

### Date and time group settings

The following table describes the date/time group settings.

**Table 5: Date/Time group settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Enter the name that you want to assign to the new date/time group.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>From the drop-down list box, choose the time zone for the group that you are adding.</td>
</tr>
<tr>
<td></td>
<td>The default setting for new Cisco Unified Communications Manager installations equals (GMT) Monrovia, Casablanca.</td>
</tr>
<tr>
<td></td>
<td>If you upgrade from a compatible Cisco Unified Communications Manager release and you use &quot;local time zone of Communications Manager&quot; in the configuration, the Cisco Unified Communications Manager database determines the appropriate time zone for the database server and then displays that time zone as replacement for the Communications Manager time zone.</td>
</tr>
<tr>
<td>Separator</td>
<td>Choose the separator character to use between the date fields.</td>
</tr>
</tbody>
</table>
Synchronize date and time group settings with devices

To synchronize devices to a date/time group that has undergone configuration changes, perform the following procedure, which applies 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 System > Date/Time Group.
The Find and List Date/Time Groups window displays.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Format</td>
<td>Choose the date format for the date that displays on the Cisco Unified IP Phones.</td>
</tr>
<tr>
<td>Time Format</td>
<td>Choose a 12-hour or 24-hour time format.</td>
</tr>
</tbody>
</table>
| Selected Phone NTP References (ordered by highest priority) | To ensure that a phone that is running SIP gets its date and time configuration from an NTP server, add the phone NTP reference(s) to the date/time group. To add a phone NTP reference to the date/time group, perform the following tasks:  
  1. Click the **Add Phone NTP References** button.  
  2. Find the phone NTP reference(s) that you want to add. Only phone NTP references that exist in the Cisco Unified Communications Manager database display.  
  3. After the search results display, check the check boxes for the phone NTP references or click **Select All**.  
  4. Click **Add Selected**.   
   After you add the phone NTP reference(s) to the date/time group, you can prioritize them, starting with the first reference that you want the phone to contact. For example, to move a reference to the top of the list, highlight the entry in the pane and click the Up arrow. To move a reference to the bottom of the list, highlight the entry in the pane and click the Down arrow.   
**Tip** To remove a phone NTP reference from the date/time group, highlight the server in the pane and click **Remove Phone NTP References**. Removing the phone NTP reference from the date/time group does not remove the phone NTP reference from the Cisco Unified Communications Manager database. |

### Related Topics

- About phone NTP reference setup, on page 43
- Date and time group setup, on page 47
Step 2  Choose the search criteria to use.
Step 3  Click Find.  
The window displays a list of Date/Time Groups that match the search criteria.
Step 4  Click the Date/Time Group to which you want to synchronize applicable devices.  
The Date/Time Group 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.

Related Topics
   Date and time group setup, on page 47
Synchronize date and time group settings with devices
CHAPTER 7

Region setup

This chapter provides information to add, update, or delete regions, and synchronize configuration changes with affected devices.

For additional information, see topics related to regions in the Cisco Unified Communications Manager System Guide, as well as topics related to Call Admission Control in the Cisco Unified Communications Manager System Guide.

- Audio Codec Preference list, page 53
- Create new Audio Codec Preference list, page 54
- Edit Audio Codec Preference list, page 54
- Delete Audio Codec Preference list, page 55
- About region setup, page 55
- Set up regions, page 56
- Region deletion, page 57
- Audio and video call bit rate settings, page 57
- Synchronize region settings with devices, page 61

Audio Codec Preference list

In Cisco Unified Communications Manager (Unified CM) Administration, use the System > Region Information > Audio Codec Preference menu path to configure the order of audio codec preference, both for calls within a region and for between regions.

Unified CM has two default Audio Codec Preference lists, one for lossy regions and another for low-loss regions. These are the Factory Default lossy, and the Factory Default low loss. Start with a default Audio Codec Preference list to create a custom list.

With the Audio Codec Preference feature, you can:

- Change the relative priorities of audio codecs.
- Save the custom Audio Codec Preference list with a unique name.
- Assign custom codec preference lists for use within a region or between regions.
Create multiple custom codec preference list.

Related Topics

Create new Audio Codec Preference list, on page 54
Edit Audio Codec Preference list, on page 54
Delete Audio Codec Preference list, on page 55

Create new Audio Codec Preference list

Procedure

Step 1 Click Add New from the Find and List Audio Codec Preference lists page. The Audio Codec Preference List Configuration page is displayed.
Step 2 Choose an Audio Codec Preference list from the dropdown list.
Step 3 Click Copy.
Step 4 In the Audio Codec Preference List Information section, enter a Name and Description.
Step 5 Place the codecs in the preferred order by using the up and down arrows.
Step 6 Click Save.

Related Topics

Edit Audio Codec Preference list, on page 54
Delete Audio Codec Preference list, on page 55

Edit Audio Codec Preference list

Procedure

Step 1 In the Audio Codec Preference lists section, click the list to be edited. The Audio Codec Preference List Configuration page is displayed.
Step 2 Reorder the audio codecs using the up and down arrows.
Step 3 Click Save.

Related Topics

Create new Audio Codec Preference list, on page 54
Delete Audio Codec Preference list, on page 55
Delete Audio Codec Preference list

Note
You cannot delete the Factory Default lossy or low loss audio codec preference lists.

Procedure

Step 1
Select the list to be deleted from the Audio Codec Preference lists section.

Step 2
Click Delete Selected.
A message box appears “You are about to permanently delete one or more Audio Codec Preference Lists. This action cannot be undone. Continue?”

Step 3
Click OK.

Related Topics
Create new Audio Codec Preference list, on page 54
Edit Audio Codec Preference list, on page 54

About region setup

In Cisco Unified Communications Manager Administration, use the System > Region menu path to configure regions.

You use regions to limit the bandwidth that is used for audio and video calls within a region and between existing regions by specifying the transport-independent maximum bit rates for audio and for video calls. You can specify the maximum bit rates for audio and video calls within a region and between existing regions.

- The maximum audio bit rate determines the codecs that are allowed for calls by filtering out codecs with bit rates that exceed the specified limit.
- The maximum video call bit rate comprises the sum of the audio and video bit rates, but does not include transport overhead.

Cisco Unified Communications Manager supports up to 2000 regions. The following limitations and restrictions apply:

- Configure as many regions as possible to Use System Default for the audio bit rate and video call bit rate fields.
- This enhancement requires an MCS 7845H1 or higher server.
- See the "Regions" subtopic under the "Administration Considerations" topic of the "IP Video Telephony" chapter of the Cisco Unified Communications Solution Reference Network Design (SRND) for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.
**Regions setup tips**

For every region, an association exists with that region in other regions; therefore, the addition of regions occurs in a matrixlike fashion. For example, if you add regions A, B, and C, a matrix with region A, region B, and region C as both columns and rows results, as shown in the following matrix:

<table>
<thead>
<tr>
<th></th>
<th>Region A</th>
<th>Region B</th>
<th>Region C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region C</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If you assign 20 regions, the database adds 400 entries (20 x 20). Some performance limitations exist when large numbers of regions are assigned.

---

**Note**

Cisco Unified Communications Manager allows you to add up to 2000 regions.

---

**Note**

Cisco recommends that you reset devices after changing a region name.

---

**Set up regions**

Follow these additional steps when configuring regions.

**Procedure**

**Step 1** To configure the settings to use within a particular region, click the name of this region to highlight it in the Regions window pane; then, configure the settings, as described in Table 6: Region settings, on page 57.

**Step 2** To configure the default codecs to use between this region and other regions, click another region name (other than this region) to highlight it in the Regions window pane. Then, configure the settings, as described in Table 6: Region settings, on page 57.

**Tip** For enhanced scalability and to conserve resources, Cisco recommends that you properly set the default values in the Clusterwide Parameters (System - Location and Region) section of the Cisco Unified Communications Manager Administration Service Parameters Configuration window for the audio codec, video call bandwidth, and link loss type values and then choose the Use System Default entries in the Cisco Unified Communications Manager Administration Region Configuration window for these fields.

**Step 3** To save the new region in the database, click **Save**.

**Tip** The Find and List Regions window displays an Rows per page drop-down list box that allows you to list 25, 50, 100, 150, 200, or 250 configured regions. If you choose to display 100 or more regions, Cisco Unified Communications Manager may experience performance degradation.
What to Do Next

After you configure a region, you can use it to configure device pools. Devices acquire a region setting from the device pool to which they are assigned.

Related Topics

Audio and video call bit rate settings, on page 57
About device pool setup, on page 63

Region deletion

You cannot delete a region that any device pools are using.

To find out which device pools use the region, choose Dependency Records from the Related Links drop-down list box on the Region Configuration window and click Go.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a region that is in use, Cisco Unified Communications Manager displays a message. Before deleting a region that is currently in use, you must perform either or both of the following tasks:

- Update the device pools to use a different region.
- Delete the device pools that use the region that you want to delete.

Tip

The Find and List Regions window displays an Items per page drop-down list box that allows you to list 25, 50, 100, 150, 200, or 250 configured regions. If you choose to display 100 or more regions, Cisco Unified Communications Manager may experience performance degradation.

Related Topics

About device pool setup, on page 63
Device pool deletion, on page 64
Access dependency records, on page 874

Audio and video call bit rate settings

The following table summarizes the audio bit rate and video call bit rate settings that can be specified for regions.

Table 6: Region settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region Information</td>
<td></td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name for this region. This name can comprise up to 30 characters. Valid characters include letters, numbers, dashes, dots (periods), blanks, and underscores.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Cisco recommends that you reset devices after changing a region name.</td>
</tr>
<tr>
<td>Region Relationships</td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td>The entries in this column display all regions for which non-default relationships have been configured.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the relationships between the region that you are configuring and this region specify only default values, this region does not display in this column.</td>
</tr>
<tr>
<td>Audio Codec Preference List</td>
<td>The entries in this column specify the audio codec preference relationship between the region that you are configuring and the region that displays in the corresponding row.</td>
</tr>
<tr>
<td>Maximum Audio Bit Rate</td>
<td>The entries in this column specify the maximum audio bit rate between the region that you are configuring and the region that displays in the corresponding row.</td>
</tr>
<tr>
<td>Maximum Session Bit Rate</td>
<td>The entries in this column specify the maximum video bit rate (including audio) between the region that you are configuring and the region that displays in the corresponding row.</td>
</tr>
<tr>
<td>for Video Calls</td>
<td></td>
</tr>
<tr>
<td>Modify Relationship to other Regions</td>
<td></td>
</tr>
<tr>
<td>Regions</td>
<td>The entries in this window pane specify all existing regions, including the Default region, the region that you are configuring, and all other regions. Choose a region in this pane prior to configuring the relationships between the region that you are configuring and the chosen region.</td>
</tr>
</tbody>
</table>
For each region that is specified in the Regions window pane, choose the corresponding value from the drop-down list box in this column to set the Audio Codec Preference list describing the network conditions between this region and the specified region. The Audio Codec Preference list determines the relative preferences for certain audio codecs, optimizing the audio quality based on whether or not the network conditions are lossy. Certain audio codecs are more robust when faced with packet loss, jitter, and delay.

Choose from the following values:

- **Keep Current Setting**—Choose this value to keep the link loss type between the region that you are configuring and the region that you specified in the Regions window pane.

- **Use System Default**—Choose this value to use the system default value for link loss type between the region that you are configuring and the region that you specified in the Regions window pane. (System default is set in the Service Parameters Configuration window.)

- **Factory Default Low Loss**—Choose this value to specify a low-loss link loss type between the region that you are configuring and the region that you specified in the Regions window pane.

- **Factory Default Lossy**—Choose this value to specify a lossy link loss type between the region that you are configuring and the region that you specified in the Regions window pane.

- **<Custom Audio Codec Preference list>**—Choose a custom Audio Codec Preference list that you have created.

**Caution**

Custom audio codec preferences must be configured identically in both clusters for H.323 Intercluster Trunks (ICTs). Inconsistent audio codec preferences may result in calls with no audio.
Foreach region that is specified in the Regions window pane, choose the value from the drop-down list box in this column to set the maximum bit rate to use for audio between this region and the specified region. This setting applies to both audio and video calls and serves as an upper limit for the audio bit rate, which means that audio codecs with higher bit rates than the one that you specify are not used for these calls.

For example, if you choose 64 kbps (G.722, G.711), G.722 or G.711 may get negotiated for the calls because both codecs use 64 kb/s. G.722 has better audio quality than G.711, so it is preferred for a call.

- Cisco recommends that you update the intraregion and interregion maximum audio bit rate service parameters. In addition, Cisco recommends that Use System Default option be chosen for this field. Configuring and using the service parameter values facilitates the modification of the Max Audio Bit Rate for many region pairs at one time.

- Because of bandwidth constraints at most remote-site deployments, use 8 kb/s (G.729) as the recommended setting between a new region and existing regions.

- If you choose Keep Current Setting, you keep the value that is specified in the Regions Relationships pane for the region pair that you are creating.

- If you choose Use System Default, the value for the Intraregion or Interregion Max Audio Bit Rate service parameter gets used, depending on the region that is selected. This service parameter supports the Cisco CallManager service.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Audio Bit Rate</td>
<td>For each region that is specified in the Regions window pane, choose the value from the drop-down list box in this column to set the maximum bit rate to use for audio between this region and the specified region. This setting applies to both audio and video calls and serves as an upper limit for the audio bit rate, which means that audio codecs with higher bit rates than the one that you specify are not used for these calls. For example, if you choose 64 kbps (G.722, G.711), G.722 or G.711 may get negotiated for the calls because both codecs use 64 kb/s. G.722 has better audio quality than G.711, so it is preferred for a call. - Cisco recommends that you update the intraregion and interregion maximum audio bit rate service parameters. In addition, Cisco recommends that Use System Default option be chosen for this field. Configuring and using the service parameter values facilitates the modification of the Max Audio Bit Rate for many region pairs at one time. - Because of bandwidth constraints at most remote-site deployments, use 8 kb/s (G.729) as the recommended setting between a new region and existing regions. - If you choose Keep Current Setting, you keep the value that is specified in the Regions Relationships pane for the region pair that you are creating. - If you choose Use System Default, the value for the Intraregion or Interregion Max Audio Bit Rate service parameter gets used, depending on the region that is selected. This service parameter supports the Cisco CallManager service.</td>
</tr>
<tr>
<td>Maximum Session Bit Rate for Video Calls</td>
<td>For each region that is specified in the Regions window pane, click one radio button in this column as specified: - Keep Current Setting—Click this button to use the current setting for the video call bandwidth. - Use System Default—Click this button to use the default value. The default value normally specifies 384 kbps, unless the default value has been set to a different value in the Service Parameters Configuration window. - None—Click this radio button if no video call bit rate is allotted between this region and the specified region. If you choose this option, the system does not allow video calls. - kbps—Click this button to set the maximum video call bit rate between the region that you are configuring and the specified region. Enter the bit rate that is available for each video call between these two regions; remember that the audio bit rate is included. Valid values range from 1 to 32256.</td>
</tr>
</tbody>
</table>
Synchronize region settings with devices

To synchronize devices with a Region that has undergone configuration changes, perform the following procedure, which applies 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 System &gt; Region. The Find and List Regions window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find. The window displays a list of Regions that match the search criteria.

**Step 4** Click the Region to which you want to synchronize applicable devices. The Find and List Regions 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.

Related Topics

Region setup, on page 53
Synchronize region settings with devices
Device pool setup

This chapter provides information to add, update, or delete a device pool.

See topics related to system-level configuration settings in the Cisco Unified Communications Manager System Guide for more information about device pools and the device settings that are assigned through device pools, as well as topics related to common device configuration.

- About device pool setup, page 63
- Device pool deletion, page 64
- Device pool settings, page 64
- Synchronize device pool settings with devices, page 79

About device pool setup

In Cisco Unified Communications Manager Administration, use the System > Device Pool menu path to configure device pools.

Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains system, device, and location-related information. The Common Device Configuration window under Device > Device Settings > Common Device Configuration records all the user-oriented information such as type of softkey template that is used and locale information. Ensure that each device is associated with a device pool and with a common device configuration for user-oriented information.

Device pool setup tips

After adding a new device pool to the database, you can use it to configure devices such as Cisco Unified IP Phones, gateways, conference bridges, transcoders, media termination points, voice-mail ports, CTI route points, and so on.

Before you configure a device pool, you must configure the following items if you want to choose them for the device pool:

- Cisco Unified Communications Manager group (required).
- Date/time group (required).
- Region (required).
• SRST reference (optional).
• Media resource group list (optional).
• Calling search space for auto-registration (optional).
• Reverted call focus priority (optional).
• Device mobility group (optional).
• Device mobility calling search space.
• Physical location (optional). See topics related to configuring a device mobility group in the Cisco Unified Communications Manager Features and Services Guide.

• Location.
• AAR group.
• AAR calling search space.

Related Topics
  About Cisco Unified Communications Manager group setup, on page 39
  About date and time group setup, on page 47
  About region setup, on page 55
  About location setup, on page 107
  About SRST reference setup, on page 115
  About AAR group setup, on page 151
  About calling search space setup, on page 247
  About media resource group list setup, on page 375

Device pool deletion

You cannot delete a device pool if any devices are assigned to it, if it is used for Device Defaults configuration, or if it is the only device pool in the database. If you try to delete a device pool that is in use, a message displays. Before deleting a device pool that is currently in use, you must perform either or both of the following tasks:

• Update the devices to assign them to a different device pool.
• Delete the devices that are assigned to the device pool that you want to delete.

Related Topics
  Phone setup, on page 539

Device pool settings

The following table lists and describes device pool settings.
### Table 7: Device pool settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Pool Settings</td>
<td></td>
</tr>
<tr>
<td>Device Pool Name</td>
<td>Enter the name of the new device pool that you are creating. You can enter up to 50 characters, which include alphanumeric characters, periods (.), hyphens (-), underscores (_), and blank spaces.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Group</td>
<td>Choose the Cisco Unified Communications Manager group to assign to devices in this device pool. A Cisco Unified Communications Manager group specifies a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager for that group, and the other members of the group serve as backup Cisco Unified Communications Managers for redundancy.</td>
</tr>
<tr>
<td>Calling Search Space for Auto-registration</td>
<td>Choose the calling search space to assign to devices in this device pool that auto-register with Cisco Unified Communications Manager. The calling search space specifies partitions that devices can search when attempting to complete a call.</td>
</tr>
<tr>
<td>Adjunct CSS</td>
<td>From the drop-down list box, choose an existing Calling Search Space (CSS) to use for the devices in this device profile as an adjunct CSS for the Extension Mobility Cross Cluster (EMCC) feature. (To configure a new CSS or modify an existing CSS, choose Call Routing &gt; Class of Control &gt; Calling Search Space in Cisco Unified Communications Manager Administration.) Default value specifies None. When configuring the EMCC feature, the administrator must configure a device pool for each remote cluster. If the remote cluster is located in a different country, the adjunct CSS must embrace the partition with which the emergency patterns of that country associate. This configuration facilitates country-specific emergency call routing. For more information about the adjunct CSS, see topics related to EMCC call routing in the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
</tbody>
</table>
### Device pool settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Reverted Call Focus Priority                    | Choose a clusterwide priority setting for reverted calls that are invoked by the hold reversion feature. This setting specifies which call type, incoming calls or reverted calls, have priority for user actions, such as going off hook.  
  - Default—If you choose this option, incoming calls have priority.  
  - Highest—If you choose this option, reverted calls have priority.  

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.  

**Note** This setting applies specifically to hold reverted calls; it does not apply to parked reverted calls.  

For more information, see topics related to hold reversion in the *Cisco Unified Communications Manager Features and Services Guide*.  

| Intercompany Media Services Enrolled Group      | Select an Intercompany Media Services Enrolled Group from the drop-down list.  
For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Roaming Sensitive Settings</td>
<td></td>
</tr>
<tr>
<td>Date/Time Group</td>
<td>Choose the date/time group to assign to devices in this device pool. The date/time group specifies the time zone and the display formats for date and time.</td>
</tr>
<tr>
<td>Region</td>
<td>Choose the Cisco Unified Communications Manager region to assign to devices in this device pool. The Cisco Unified Communications Manager region settings specify voice codec that can be used for calls within a region and between other regions.</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>From the drop-down list box, choose a media resource group list. A media resource group list specifies a prioritized list of media resource groups. An application selects the required media resource (for example, a music on hold server, transcoder, or conference bridge) from the available media resource groups according to the priority order that is defined in a media resource group list.</td>
</tr>
</tbody>
</table>
Device pool settings

<table>
<thead>
<tr>
<th>Field Name</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 device pool. A location setting of None or Hub_None means that the locations feature does not keep track of the bandwidth that the devices in this device pool consume. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the System &gt; Location menu option. For an explanation of location-based CAC across intercluster trunks, see topics related to location-based CAC in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Network Locale</td>
<td>From the drop-down list box, choose the locale that is associated with phones and gateways. The network locale contains a definition of the tones and cadences that the phones and gateways in the device pool in a specific geographic area use. Make sure that you select a network locale that is supported by all of the phones and gateways that use this device pool. If the user does not choose a network locale, the locale that is specified in the Cisco Unified Communications Manager clusterwide parameters as Default Network Locale applies. Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If a device is associated with a network locale that it does not support in the firmware, the device will fail to come up.</td>
</tr>
<tr>
<td>SRST Reference</td>
<td>From the drop-down list box, choose a survivable remote site telephony (SRST) reference to assign to devices in this device pool. Choose from the following options: - Disable—if you choose this option, devices in this device pool will not have SRST reference gateways that are available to them. - Use Default Gateway—if you choose this option, devices in this device pool use the default gateway for SRST. - Existing SRST references—if you choose an SRST reference from the drop-down list, devices in this device pool will use this SRST reference gateway.</td>
</tr>
</tbody>
</table>
### Field Name | Description
---|---
Connection Monitor Duration | This setting defines the time that the Cisco Unified IP Phone monitors its connection to Cisco Unified Communications Manager before it unregisters from SRST and reregisters to Cisco Unified Communications Manager. To use the configuration for the enterprise parameter, you can enter -1 or leave the field blank. The default value for the enterprise parameter equals 120 seconds. Change this setting if you need to disable the connection monitor or if you want to extend the connection monitor time. The maximum number of seconds that you can enter in the field equals 2592000. **Tip** When you change the value of the connection monitor duration, it applies only to the device pool that is being updated. All other device pools use the value in their own connection monitor duration fields or use the value that is configured in the enterprise parameter. For more information, see topics related to survivable remote site telephony in the *Cisco Unified Communications Manager System Guide*.  
Single Button Barge | This setting determines whether the devices or phone users in this device pool have single-button access for barge and cBarge. From the drop-down list box, choose from the following options:  
  - Off—If you choose this option, the devices in this device pool will have the Single Button Barge/cBarge feature disabled.  
  - Barge—If you choose this option, the devices in this device pool will have the Single Button Barge feature enabled.  
  - cBarge—If you choose this option, the devices in this device pool will have the Single Button cBarge feature enabled.  
  - Default—If you choose this option, the devices in this device pool will use the service parameter setting for the Single Button Barge/cBarge feature.  
Join Across Lines | This setting determines whether the Join Across Lines feature is enabled for the devices or phone users in this device pool. From the drop-down list box, choose from the following options:  
  - Off—If you choose this option, the devices in this device pool will have the Join Across Lines feature disabled.  
  - On—If you choose this option, the devices in this device pool will have the Join Across Lines feature enabled.  
  - Default—If you choose this option, the devices in this device pool will use the service parameter setting for the Join Across Lines feature.  
Physical Location | Select the physical location for this device pool. The system uses physical location with the device mobility feature to identify the parameters that relate to a specific geographical location.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Mobility Group</td>
<td>Device mobility groups represent the highest level geographic entities in your network and are used to support the device mobility feature.</td>
</tr>
<tr>
<td>Device Mobility Related</td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Device Mobility Calling Search</td>
<td>Choose the appropriate calling search space to be used as the device calling search space when the device is roaming and in same device mobility group.</td>
</tr>
<tr>
<td>Space</td>
<td></td>
</tr>
<tr>
<td>AAR Calling Search Space</td>
<td>Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.</td>
</tr>
<tr>
<td>AAR Group</td>
<td>Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.</td>
</tr>
<tr>
<td>Calling Party Transformation</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 pool.</td>
</tr>
<tr>
<td>CSS</td>
<td></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 Calling Party Transformation CSS as None for the device pool and you check the Use Device Pool Calling Party Transformation CSS check box in the device configuration window, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.</td>
</tr>
<tr>
<td>Called Party Transformation</td>
<td>This setting allows you to localize the called party number on the device. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool.</td>
</tr>
<tr>
<td>CSS</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing.</td>
</tr>
<tr>
<td>Geolocation Configuration</td>
<td></td>
</tr>
</tbody>
</table>
### Geolocation

From the drop-down list box, choose a geolocation.

You can choose the Unspecified geolocation, which designates that the devices in this device pool do not associate with a geolocation.

You can also choose a geolocation that has been configured with the **System > Geolocation Configuration** menu option.

For an explanation of geolocations, including configuration details, see topics related to geolocations and location conveyance in the *Cisco Unified Communications Manager Features and Services Guide*.

For an overview and details of how logical partitioning uses geolocations, see topics related to geolocations and location conveyance in the *Cisco Unified Communications Manager Features and Services Guide*.

---

### Geolocation Filter

From the drop-down list box, choose a geolocation filter.

If you leave the <None> setting, no geolocation filter gets applied for the devices in this device pool.

You can also choose a geolocation filter that has been configured with the **System > Geolocation Filter** menu option.

For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.

---

### Incoming Calling Party Settings

- **Clear Prefix Settings**
  - To delete all prefixes for all calling party number types, click Clear Prefix Settings.

- **Default Prefix Settings**
  - To enter the default value for all prefix fields at the same time, click Default Prefix Settings.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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. If the word, Default, displays in the Prefix field, 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, up to the number 24, 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>• 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. 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>
<tr>
<td></td>
<td><strong>Tip</strong> For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>
Configure the following settings to globalize calling party numbers that use International 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 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. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes.

- **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.

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.

**Tip** For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide*.

---

<table>
<thead>
<tr>
<th>Field Name</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. 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, up to the number 24, 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>• 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. 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>
<tr>
<td></td>
<td>For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th>Field Name</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 (#). 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, up to the number 24, 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>• 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. 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>

**Tip** For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide.*
### 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 (#).
  
  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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes.

- **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. 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.

**Tip** For more information on configuring these settings, see topics related to configuring incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide*.

### Incoming Called Party Settings

The Incoming Called Party Settings support H.323 trunks and gateways. The H.323 protocol does not support the international escape character +. To ensure the correct prefixes, including the +, get applied to inbound calls over H.323 gateways/trunks, configure the incoming called party settings; that is, configuring the incoming called party settings ensures that when an inbound call comes from a H.323 gateway or H.323 trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Prefix Settings</td>
<td>To delete all prefixes for all called party number types, click Clear Prefix Settings.</td>
</tr>
<tr>
<td>Default Prefix Settings</td>
<td>To enter the default value for all prefix fields at the same time, click Default Prefix Settings.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>National Number</td>
<td>Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type.</td>
</tr>
<tr>
<td></td>
<td>• Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 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>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 called party prefix, which supports both the prefix and strip digit functionality.</td>
</tr>
<tr>
<td></td>
<td>Tip To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of National type before it applies the prefixes.</td>
</tr>
<tr>
<td></td>
<td>• Calling Search Space—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.</td>
</tr>
</tbody>
</table>
Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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 called party prefix, which supports both the prefix and strip digit functionality.

  **Tip**  To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field.

- **Strip Digits**—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes.

- **Calling Search Space**—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Number</td>
<td>Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type.</td>
</tr>
<tr>
<td></td>
<td>• Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 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>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 called party prefix, which supports both the prefix and strip digit functionality.</td>
</tr>
<tr>
<td></td>
<td>Tip To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of Unknown type before it applies the prefixes.</td>
</tr>
<tr>
<td></td>
<td>• Calling Search Space—This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.</td>
</tr>
</tbody>
</table>
Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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 called party prefix, which supports both the prefix and strip digit functionality.

**Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field.

- **Strip Digits**—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Subscriber type before it applies the prefixes.

- **Calling Search Space**—This setting allows you to transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

### Phone Settings

#### Calling Party Transformation CSS

From the drop-down list box, choose the Calling Search Space that contains the Calling Party Transformation Pattern that you want to apply to devices in this device pool.

When Cisco Unified CM receives a call from a device in this device pool on an inbound line, Cisco Unified CM immediately applies the calling party transformation patterns in this CSS to the digits in the calling party number before it routes the call. This setting allows you to apply digit transformations to the calling party number before Cisco Unified CM routes the call. For example, a transformation pattern can change a phone extension to appear as an E.164 number.
Redirecting Party Settings

This setting allows you to transform the redirecting party number on the device to E164 format. Cisco Unified Communications Manager includes the transformed number in the diversion header of invite messages for SIP trunks and in the Redirecting Number Information Element of setup message (for H.323 and MGCP) sent out of Cisco Unified Communications Manager. Make sure that the Redirecting Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device pool.

**Note** If you configure the Redirecting Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.

### Synchronize device pool settings with devices

To synchronize devices to a device pool that has undergone configuration changes, perform the following procedure, which applies 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 **System > Device Pool**. The Find and List Device Pools window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find. The window displays a list of Device Pools that match the search criteria.

**Step 4** Click the Device Pool to which you want to synchronize applicable devices. The Device Pool 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.
Synchronize device pool settings with devices
This chapter contains information about DHCP server configuration.

For additional information, see topics related to Dynamic Host Configuration Protocol in the *Cisco Unified Communications Manager System Guide*.

- About DHCP server setup, page 81
- DHCP server deletion, page 81
- DHCP server settings, page 81
- Activate DHCP monitor service, page 83
- Start DHCP monitor service, page 83

### About DHCP server setup

In Cisco Unified Communications Manager Administration, use the **System > DHCP > DHCP Server** menu path to configure a DHCP server.

Dynamic Host Configuration Protocol (DHCP) server enables Cisco Unified IP Phones, connected to either the customer's data or voice Ethernet network, to dynamically obtain their IP addresses and configuration information. DHCP uses Domain Name System (DNS) to resolve host names both within and outside the cluster.

### DHCP server deletion

If the DHCP server is not in use, Cisco Unified Communications Manager allows you to delete the server. If the server is in use, an error message displays.

### DHCP server settings

The following table describes the DHCP server settings.
### Table 8: DHCP server settings

<table>
<thead>
<tr>
<th>Server Information Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Server</td>
<td>Select a host server from the drop-down list of available host servers.</td>
</tr>
<tr>
<td>Primary DNS IPv4 Address</td>
<td>This field specifies primary DNS IPv4 address.</td>
</tr>
<tr>
<td>Secondary DNS IPv4 Address</td>
<td>This field specifies secondary DNS IPv4 address.</td>
</tr>
<tr>
<td>Primary TFTP Server IPv4 Address (Option 150)</td>
<td>You can enable the IP phones to access the TFTP server using DHCP custom option 150. This is the method that Cisco recommends.</td>
</tr>
<tr>
<td></td>
<td>This field specifies the IPv4 address for primary Trivial File Transfer Protocol (TFTP) server.</td>
</tr>
<tr>
<td>Secondary TFTP Server IPv4 Address (Option 150)</td>
<td>This field specifies the IPv4 address for secondary TFTP server.</td>
</tr>
<tr>
<td>Bootstrap Server IPv4 Address</td>
<td>This field specifies the address of the server that is used in the next step of the bootstrap process. You can use as the IPv4 address of the TFTP server or as the default value to DHCP server address if the server supplies the next bootstrap service.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The Domain Name specifies the domain name that you should use when resolving hostname via the Domain Name System.</td>
</tr>
<tr>
<td>TFTP Server Name (Option 66)</td>
<td>You can enable the IP phones to access the TFTP server by using DHCP option 66. Use this field to identify a TFTP server. You can configure only one DNS name or a dotted decimal IP address in this parameter.</td>
</tr>
<tr>
<td>ARP Cache Timeout</td>
<td>This field specifies the timeout in seconds for ARP cache entries. Specify the time as a 32-bit unsigned integer. The default for the Cisco Network Registrar (CNR) DHCP server specifies 60 seconds.</td>
</tr>
<tr>
<td>IP Address Lease Time</td>
<td>The DHCP server uses the information in this field to specify the lease time that it is willing to offer. Specify the time in units of seconds and as a 32-bit unsigned integer. The default for the CNR DHCP server specifies seven days (604,800 seconds).</td>
</tr>
<tr>
<td>Renewal(T1) Time (sec)</td>
<td>This field specifies the time interval from address assignment until the client transitions to the RENEWING state. Typically, set this field to half the value of the IP address lease time. For example, if the IP address lease time is typically set to 60,000 seconds, the renewal time gets set to 30,000 seconds.</td>
</tr>
</tbody>
</table>
### Server Information Field

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebinding (T2) Time (sec)</td>
<td>This field specifies the time interval from address assignment until the client transitions to the REBINDING state. Specify the value in units of seconds and as a 32-bit unsigned integer. Typically, set this field to approximately 75 percent of the value of the IP address lease time. For example, if the IP address lease time is set to 60,000 seconds, the re-binding time typically gets set to about 45,000 seconds. In Windows, 85 percent of the value of the IP address lease time represents the standard.</td>
</tr>
</tbody>
</table>

### Activate DHCP monitor service

You can activate and deactivate DHCP monitor process by using the Serviceability window of Cisco Unified Communications Manager. Use the following procedure to activate the service.

**Procedure**

1. **Step 1**  
   From Cisco Unified Serviceability, choose **Tools > Service Activation**. The Service Activation window displays.

2. **Step 2**  
   Choose the Cisco Unified Communications Manager server from the Servers drop-down list box and click Go.

3. **Step 3**  
   Choose Cisco DHCP Monitor Service from the CM Services list and click Save.  
   **Note**  
   If the service is already activated, the Activation Status will display as Activated.

4. **Step 4**  
   The service gets activated, and the Activation Status column displays the status as Activated.  
   **Note**  
   The DHCP monitor service starts automatically after it is activated.

### Start DHCP monitor service

The DHCP Monitor Service starts automatically after it is activated by using Cisco Unified Serviceability. This section describes the procedures to stop or restart the DHCP service.

**Procedure**

1. **Step 1**  
   In Cisco Unified Serviceability, choose **Tools > Control Center - Feature Services**.
The Control Center—Feature Services window displays.

**Step 2**  
Choose the Cisco Unified Communications Manager server from the Servers drop-down list box and click Go.  
Cisco DHCP Monitor Service displays in the list under Service Name column, in Unified CM Services.  

*Note*  
The Activation Status displays as Activated if you followed the procedure to active the DHCP monitor service.

**Step 3**  
Check the radio button corresponding to Cisco DHCP Monitor Service.

**Step 4**  
If you want to restart the Cisco DHCP Monitor Service, click Restart.  
The service restarts, and the message, Service Successfully Restarted, displays.

**Step 5**  
If you want to stop the Cisco DHCP Monitor Service, click Stop.  
The service stops, and the message, Service Successfully Stopped, displays.

**Step 6**  
If you want to start a stopped Cisco DHCP Monitor Service, click Start.  
The service starts, and the message, Cisco DHCP Monitor Service Restarted Successfully, displays.

---

**Related Topics**

- DHCP server setup, on page 81
- Activate DHCP monitor service, on page 83
DHCP subnet setup

This chapter describes the procedures for adding subnets to DHCP servers. Use the following procedures to find and add subnets to DHCP servers:

For additional information, see topics related to Dynamic Host Configuration Protocol in the Cisco Unified Communications Manager System Guide.

- About DHCP subnet setup, page 85
- DHCP subnet deletion, page 85
- DHCP subnet settings, page 85

About DHCP subnet setup

In Cisco Unified Communications Manager Administration, use the System > DHCP Subnet menu path to configure DHCP subnets.

**DHCP subnet setup tips**

Changes to the server configuration do not take effect until you restart Cisco Unified Communications Manager. For information about restarting the Cisco CallManager service, see the Cisco Unified Serviceability Administration Guide.

DHCP subnet deletion

If the subnet is not in use, Cisco Unified Communications Manager allows you to delete it. If the subnet is in use, a message displays.

DHCP subnet settings

In the DHCP Subnet Configuration window, you can add subnets to the DHCP server. The following table describes the DHCP subnet settings.
### Table 9: DHCP subnet settings

<table>
<thead>
<tr>
<th>DHCP Subnet Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>Choose the DHCP server name from the drop-down list box.</td>
</tr>
<tr>
<td>Subnet IPv4 Address</td>
<td>Enter the Subnet IPv4 address.</td>
</tr>
<tr>
<td>Primary Start IPv4 Address</td>
<td>Enter the start IPv4 address of the first range of IP addresses to be assigned.</td>
</tr>
<tr>
<td>Primary End IPv4 Address</td>
<td>Enter the end IPv4 address of the first range of IP addresses to be assigned.</td>
</tr>
<tr>
<td>Secondary Start IPv4 Address</td>
<td>Enter the start IPv4 address of the second range of IP addresses to be assigned.</td>
</tr>
<tr>
<td>Secondary End IPv4 Address</td>
<td>Enter the end IPv4 address of the second range of IP addresses to be assigned.</td>
</tr>
<tr>
<td>Primary Router IPv4 Address</td>
<td>Enter the IPv4 address of the primary router on your subnet.</td>
</tr>
<tr>
<td>Secondary Router IPv4 Address</td>
<td>Enter the IPv4 address of the secondary router on your subnet.</td>
</tr>
<tr>
<td>IPv4 Subnet Mask</td>
<td>Enter the subnet mask.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>This field specifies the name that you should use when resolving hostname via the Domain Name System.</td>
</tr>
<tr>
<td>Primary DNS IPv4 Address</td>
<td>This field specifies primary DNS IPv4 server name.</td>
</tr>
<tr>
<td>Secondary DNS IPv4 Address</td>
<td>This field specifies secondary DNS IPv4 server name.</td>
</tr>
<tr>
<td>TFTP Server Name (Option 66)</td>
<td>Use this field to identify a TFTP server. You can configure only one DNS name or a dotted decimal IP address in this parameter.</td>
</tr>
<tr>
<td>Primary TFTP Server IPv4 Address (Option 150)</td>
<td>This field specifies the IPv4 addresses for primary Trivial File Transfer Protocol (TFTP) server.</td>
</tr>
<tr>
<td>Secondary TFTP Server IPv4 Address (Option 150)</td>
<td>This field specifies the IPv4 addresses for secondary TFTP server.</td>
</tr>
<tr>
<td>Bootstrap Server IPv4 Address</td>
<td>This field specifies the address of the server that is used in the next step of the bootstrap process. You can use this as the IPv4 address of the TFTP server or as the default value to DHCP server address if the server is to supply the next bootstrap service.</td>
</tr>
<tr>
<td>ARP Cache Timeout (sec)</td>
<td>This field specifies the timeout in seconds for ARP cache entries. Specify the time as a 32-bit unsigned integer.</td>
</tr>
<tr>
<td>IP Address Lease Time (sec)</td>
<td>The DHCP server uses the information in this field to specify the lease time that it is willing to offer. Specify the time in units of seconds and as a 32-bit unsigned integer.</td>
</tr>
</tbody>
</table>
DHCP Subnet Information | Description
---|---
Renewal (T1) Time (sec) | This field specifies the time interval from address assignment until the client transitions to the RENEWING state.
Rebinding (T2) Time (sec) | This field specifies the time interval from address assignment until the client transitions to the REBINDING state. Specify the value in units of seconds and as a 32-bit unsigned integer.

Related Topics

DHCP subnet setup, on page 85
DHCP subnet settings
LDAP system setup

This chapter provides information to configure LDAP system parameters using Cisco Unified Communications Manager. The LDAP directory configuration takes place in the following windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

For additional information, see topics related to the directory, application users, and end users in the Cisco Unified Communications Manager System Guide.

- About LDAP System setup, page 89
- LDAP system settings, page 90

About LDAP System setup

In Cisco Unified Communications Manager Administration, use the System > LDAP > LDAP System menu path to configure LDAP system settings.

Use the LDAP System Configuration window to enable LDAP synchronization and to set up the LDAP server type and the LDAP attribute name for the user ID.

Before you begin

The setting of the Enable Synchronizing from LDAP Server check box in this window affects the ability to modify end users in Cisco Unified Communications Manager Administration. LDAP synchronization applies only to end users; LDAP synchronization does not affect application users. See topics related to understanding the directory in the Cisco Unified Communications Manager System Guide for more information about LDAP synchronization.

For end user data, you cannot use the End User Configuration window to update the attributes that get synchronized from the corporate directory. You can update these attributes only in the corporate directory itself, after which you should perform a resynchronization.
You can make changes to LDAP Directory information and LDAP Authentication settings only if synchronization from the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

**Note**
If end users exist in the Cisco Unified Communications Manager database before synchronization with a corporate directory occurs, the system will delete those end users that did not have a matching user ID in the corporate directory. For example, if users bob and sanjay were in the Cisco Unified Communications Manager database, but only bob was in the LDAP directory, then sanjay would be marked inactive and eventually get deleted by the garbage collector program.

**Note**
After an LDAP Directory configuration for the DirSync service gets created or the LDAP user authentication is enabled, the settings in the LDAP System Configuration window become read only.

**Note**
After you configure LDAP synchronization in Cisco Unified Communications Manager Administration, users without last names in the corporate directory do not synchronize with the Cisco Unified Communications Manager database. No error displays in Cisco Unified Communications Manager Administration, but the log file indicates which users did not synchronize.

### LDAP system settings

The following table describes the LDAP system settings.

**Table 10: LDAP system settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP System Information</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Synchronizing from LDAP Server</td>
<td>To enable synchronization of data from the customer LDAP server, check this check box.</td>
</tr>
<tr>
<td></td>
<td>If synchronization with the LDAP server is enabled, the following circumstances occur:</td>
</tr>
<tr>
<td></td>
<td>• You cannot modify end user data, except for the fields (attributes) that are not synchronized from the corporate directory. Example: user PIN. (The administrator can always modify application user data.)</td>
</tr>
<tr>
<td></td>
<td>• You can modify the LDAP Directory information.</td>
</tr>
<tr>
<td></td>
<td>• You can modify LDAP Authentication information.</td>
</tr>
<tr>
<td></td>
<td>If synchronization with the LDAP server is not enabled (is disabled), the following circumstances occur:</td>
</tr>
<tr>
<td></td>
<td>• You cannot modify LDAP Directory information.</td>
</tr>
<tr>
<td></td>
<td>• You cannot modify LDAP Authentication information.</td>
</tr>
<tr>
<td>LDAP Server Type</td>
<td>If synchronization with the LDAP server is currently enabled, you can choose one of the selections in this drop-down list box. Choose the value that corresponds to the customer LDAP server type:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Active Directory Application Mode</td>
</tr>
<tr>
<td></td>
<td>• Netscape or Sun ONE LDAP Server</td>
</tr>
<tr>
<td></td>
<td>• OpenLDAP</td>
</tr>
</tbody>
</table>
If synchronization with the LDAP server is enabled, you can choose an LDAP attribute value for the user ID. Choose one of the following values from the drop-down list box:

- **For Microsoft Active Directory**
  * sAMAccountName
  * mail
  * employeeNumber
  * telephoneNumber
  * userPrincipalName

- **For Microsoft Active Directory Application Mode**
  * uid
  * mail
  * employeeNumber
  * telephoneNumber
  * userPrincipalName

- **For Sun ONE LDAP Server, iPlanet, and OpenLDAP**
  * uid
  * mail
  * employeeNumber
  * telephoneNumber

### Related Topics

LDAP system setup, on page 89
CHAPTER 12

LDAP directory setup

This chapter provides information to configure the LDAP directory. The LDAP directory configuration takes place in these related windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

For additional information, see topics related to the directory, application users, and end users in the Cisco Unified Communications Manager System Guide.

- About LDAP directory setup, page 93
- LDAP directory settings, page 94

About LDAP directory setup

In Cisco Unified Communications Manager, use the System > LDAP > LDAP Directory menu path to configure LDAP directories.

In the LDAP Directory window, you specify information about the LDAP directory; for example, the name of the LDAP directory, where the LDAP users exist, how often to synchronize the data, and so on.

When LDAP synchronization happens, users get added to the Cisco Unified Communications Manager and are assigned with extensions. With the introduction of Self-Provisioning, changes to a users primary telephone number in LDAP are synced to the user. However, the extension that was assigned based upon mask and the old primary number is not updated with the new number. And, deleting the user does not delete the extension, thus retaining the extension on the phone that it was assigned to.
Assuming LDAP data is accurate, during LDAP synchronization, and using the mask, extensions are created based on the desired requirements. If LDAP data is not accurate, it can create undesired extensions and can affect dial plan and routing that can lead to outside dial tones to fail, or be delayed, or some other numbers to not be reachable. Ensure that LDAP data is always accurate to avoid changes in dial plans and routing behavior.

Before you begin

Before you can synchronize the LDAP directory, you must activate the Cisco DirSync service. For information about how to activate services, see the Cisco Unified Serviceability Administration Guide.

Changes to LDAP Directory information and LDAP Authentication settings are possible only if synchronization from the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

LDAP directory settings

The following table describes the LDAP directory settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Directory Information</td>
<td></td>
</tr>
<tr>
<td>LDAP Configuration Name</td>
<td>Enter a unique name (up to 40 characters) for the LDAP directory.</td>
</tr>
<tr>
<td>LDAP Manager Distinguished Name</td>
<td>Enter the user ID (up to 128 characters) of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory in question.</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>Enter a password (up to 128 characters) for the LDAP Manager.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Reenter the password that you provided in the LDAP Password field.</td>
</tr>
<tr>
<td>LDAP User Search Base</td>
<td>Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup.</td>
</tr>
</tbody>
</table>
### LDAP Custom Filter

Select an LDAP custom filter from the drop-down list. The LDAP filter filters the results of LDAP searches. LDAP users that match the filter get imported into the Cisco Unified Communications Manager database, but LDAP users that do not match the filter do not get imported.

The default value is `<None>`. This value applies a default LDAP filter that is specific to the LDAP server type. These are the default LDAP filters:

- **Microsoft Active Directory (AD):**
  
  \((\&(&\text{objectclass}\text{-}\text{user})(!(\text{objectclass}\text{-}\text{Computer}))
  \((!(\text{UserAccountControl}\text{-}1.2.840.113556.1.4.803\text{-}2)))\))

- **iPlanet or Sun One LDAP Server:**
  
  \((\text{objectclass}\text{-}\text{inetOrgPerson})\)

- **OpenLDAP:**
  
  \((\text{objectclass}\text{-}\text{inetOrgPerson})\)

- **Microsoft Active Directory Application Mode (ADAM):**
  
  \((\&(&\text{objectclass}\text{-}\text{user})
  \((!(\text{msDS}\text{-}\text{-UserAccountDisabled}\text{-}\text{TRUE}))\))\)

For more information about LDAP filters, see the [LDAP custom filter setup](#), on page 105.

### LDAP Directory Synchronization Schedule

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform Sync Just Once</td>
<td>If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified Communications Manager database only once, check this check box.</td>
</tr>
<tr>
<td>Perform a Re-sync Every</td>
<td>If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified Communications Manager database at a regular interval, use these fields. In the left field, enter a number. In the drop-down list box, choose a value:</td>
</tr>
<tr>
<td></td>
<td>• hours</td>
</tr>
<tr>
<td></td>
<td>• days</td>
</tr>
<tr>
<td></td>
<td>• weeks</td>
</tr>
<tr>
<td></td>
<td>• months</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager can synchronize directory information every 6 hours, which is the minimum value allowed for this field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field remains active only if you do not check the Perform Sync Just Once check box.</td>
</tr>
<tr>
<td>Next Re-sync Time (YYYY-MM-DD hh:mm)</td>
<td>Specify a time to perform the next synchronization of Cisco Unified Communications Manager directory data with this LDAP directory. Use a 24-hour clock to specify the time of day. For example, 1:00 pm equals 13:00.</td>
</tr>
</tbody>
</table>
## LDAP directory settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard User Fields To Be Synchronized</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Unified Communications Manager User Fields</strong></td>
<td><strong>LDAP User Fields</strong></td>
</tr>
<tr>
<td>User ID</td>
<td>sAMAccountNameoruid</td>
</tr>
<tr>
<td>Middle Name</td>
<td>(drop-down list box)</td>
</tr>
<tr>
<td></td>
<td>For the LDAP User field, choose one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• middleName</td>
</tr>
<tr>
<td></td>
<td>• initials</td>
</tr>
<tr>
<td>Manager ID</td>
<td>manager</td>
</tr>
<tr>
<td>Directory URI</td>
<td>(drop-down list box)</td>
</tr>
<tr>
<td></td>
<td>For the LDAP User field, choose one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• msRTCSIP-primaryuseraddress</td>
</tr>
<tr>
<td></td>
<td>• mail</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The msRTCSIP-primaryuseraddress option is only available if you choose Microsoft Active Directory as the LDAP Server Type in the LDAP System Configuration window.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>By default, the user portion of a directory URI is case-sensitive. Under this setting, whatever case the directory URI has in LDAP will be imported into Cisco Unified Communications Manager. For compatibility with third party call control systems, Cisco recommends that you change this setting by setting the value of the URI Lookup Policy enterprise parameter to case-insensitive.</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
</tr>
<tr>
<td>Department</td>
<td>departmentordepartmentnumber</td>
</tr>
<tr>
<td>Mail ID</td>
<td>(drop-down list box)</td>
</tr>
<tr>
<td>Custom User Fields To Be Synchronized</td>
<td></td>
</tr>
</tbody>
</table>

**Custom User Field Name**

- Cisco Unified Communications Manager allows you to synchronize LDAP directory attributes that are not included among the defaults for the Standard User Fields to be Synchronized. Using Custom User Fields, you can synchronize LDAP attributes to a customized field that gets saved in the Cisco Unified Communications Manager database.

- In the Custom User Field text box, enter a name for the customized field that you want to create. The custom user field can contain up to 64 alphanumeric characters, including spaces. Cisco Unified Communications Manager saves the new customized field in the database.

- You can create up to five custom user fields. Click the (+) button to add additional rows on which you can create new fields.

**LDAP Attribute**

- In the LDAP attribute field, enter a valid LDAP attribute that exists in your LDAP directory. The maximum field length is 128 characters.

**LDAP Server Information**

<p>| Host Name or IP Address for Server | Enter the host name or IP address of the server where the data for this LDAP directory resides.                                                                                                                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| LDAP Port                           | Enter the port number on which the corporate directory receives the LDAP requests. You can only access this field if LDAP authentication for end users is enabled. The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636. How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:

**LDAP Port when LDAP server is not a Global Catalog server:**
- 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.)
- 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

**LDAP Port when LDAP server is a Global Catalog server:**
- 3268—When SSL is not required.
- 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

**Tip** Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter. |
| Use SSL                             | Check this check box to use Secured Sockets Layer (SSL) encryption for security purposes. **Note** If LDAP over SSL is required, the corporate directory SSL certificate must be loaded into Cisco Unified Communications Manager. The *Cisco Unified Communications Operating System Administration Guide* documents the certificate upload procedure in the Security chapter.                                                                                      |
| Add Another Redundant LDAP Server   | Click this button to add another row for entry of information about an additional server.                                                                                                                                                                                                                                                                                                                                                                                |
| Perform Full Sync                   | Click this button to perform a full directory sync. While the directory is synchronizing, the button name changes to Cancel Full Sync. You can click the Cancel Full Sync button to cancel the sync.                                                                                                                                                                                                                           |
In addition to the user fields that appear in Cisco Unified Communications Manager Administration, the Microsoft Active Directory Application Mode user fields that are described in the following table also get synchronized.

**Table 12: Additional synchronized Microsoft Active Directory Application Mode user fields**

<table>
<thead>
<tr>
<th>Cisco Unified Communications Manager User Fields</th>
<th>LDAP User Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>UniqueIdentifier</td>
<td>ObjectGUID</td>
</tr>
<tr>
<td>Pager</td>
<td>pagerorpagertelephonenumber</td>
</tr>
<tr>
<td>Mobile</td>
<td>mobileormobiletelephonenumber</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
</tr>
<tr>
<td>Homephone</td>
<td>homephoneorhometelephonenumber</td>
</tr>
<tr>
<td>OCSPrimaryUserAddress</td>
<td>msRTCSIP-primaryuseraddress</td>
</tr>
</tbody>
</table>
CHAPTER 13

LDAP authentication setup

This chapter provides information to configure LDAP directory, authentication, and custom filters using Cisco Unified Communications Manager. The LDAP directory configuration takes place in the following windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

You can make changes to LDAP directory information and LDAP authentication settings only if synchronization with the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

For additional information, see topics related to the directory, application users, and end users in the Cisco Unified Communications Manager System Guide.

- About LDAP authentication setup, page 101
- Update LDAP authentication, page 102
- LDAP authentication settings, page 102

About LDAP authentication setup

In Cisco Unified Communications Manager Administration, use the System > LDAP > LDAP Authentication menu path to configure LDAP authentication.

The authentication process verifies the identity of the user by validating the user ID and password/PIN before granting access to the system. Verification takes place against the Cisco Unified Communications Manager database or the LDAP corporate directory.

You can only configure LDAP authentication if you enable LDAP synchronization in the LDAP System Configuration window.
User accounts must be synchronized with Cisco Unified Communications Manager to use LDAP authentication. Administrators must enable LDAP synchronization and configure LDAP directory instance(s) to use the LDAP authentication mechanism.

When both synchronization and LDAP authentication are enabled, the system always authenticates application users and end user PINs against the Cisco Unified Communications Manager database. End user passwords get authenticated against the corporate directory; thus, end users need to use their corporate directory password.

When only synchronization is enabled (and LDAP authentication is not enabled), end users get authenticated against the Cisco Unified Communications Manager database. In this case, the administrator can configure a password in the End User Configuration window in Cisco Unified Communications Manager Administration.

## Update LDAP authentication

The setting of the Enable Synchronizing from LDAP Server check box in the LDAP System Configuration window affects your ability to modify LDAP authentication settings. If synchronization with the LDAP server is enabled, you cannot modify LDAP directory information and LDAP authentication settings. See topics related to understanding the directory in the Cisco Unified Communications Manager System Guide for more information about LDAP synchronization.

Conversely, if you want to enable administrators to modify LDAP directory information and LDAP authentication settings, you must disable synchronization with the LDAP server.

### LDAP authentication settings

The following table describes the LDAP authentication settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| LDAP Authentication for End Users | Click this check box to require authentication of end users from the LDAP directory. If the check box is left unchecked, authentication gets performed against the database.  
**Note** You can only access this field if LDAP synchronization is enabled in the LDAP System Configuration window. |
| Use LDAP Authentication for End Users | Enter the user ID of the LDAP Manager who is an administrative user that has access rights to the LDAP directory in question.  
**Note** You can only access this field if LDAP authentication for end users is enabled. |
| LDAP Manager Distinguished Name | Enter a password for the LDAP Manager.  
**Note** You can only access this field if LDAP authentication for end users is enabled. |
Confirm Password: Reenter the password that you provided in the LDAP Password field.  
*Note:* You can only access this field if LDAP authentication for end users is enabled.

LDAP User Search Base: Enter the user search base. Cisco Unified Communications Manager searches for users under this base.  
*Note:* You can only access this field if LDAP authentication for end users is enabled.

**LDAP Server Information**

Host Name or IP Address for Server: Enter the host name or IP address where you installed the corporate directory.  
*Note:* You can only access this field if LDAP authentication for end users is enabled.

LDAP Port: Enter the port number on which the corporate directory receives the LDAP requests. You can only access this field if LDAP authentication for end users is enabled.

The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636.

How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:

**LDAP port when LDAP server is not a Global Catalog server:**

- **389**—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.)
- **636**—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

**LDAP port when LDAP server is a Global Catalog server:**

- **3268**—When SSL is not required.
- **3269**—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

**Tip:** Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.
**Use SSL**
Check this check box to use SSL encryption for security purposes.

**Note** If LDAP over SSL is required, the corporate directory SSL certificate must be loaded into Cisco Unified Communications Manager. The *Cisco Unified Communications Operating System Administration Guide* describes the certificate upload procedure.

If you check the Use SSL check box, enter the IP address or the hostname that exists in the corporate directory SSL certificate in the Host Name or IP Address for Server field in the LDAP Authentication Configuration window. If the certificate contains an IP address, enter the IP address. If the certificate contains the hostname, enter the hostname. If you do not enter the IP address or hostname exactly as it exists in the certificate, problems may occur for some applications; for example, applications that use CTIManager.

**Add Another Redundant LDAP Server**
Click this button to add another row for entry of information about an additional server.

**Note** You can only access this button if LDAP authentication for end users is enabled.
This chapter provides information to configure the LDAP directory. Configuration takes place in these related windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

For additional information, see topics related to the directory, application users, and end users in the Cisco Unified Communications Manager System Guide.

- About LDAP custom filter setup, page 105
- LDAP filter deletion, page 106
- LDAP filter settings, page 106

### About LDAP custom filter setup

In Cisco Unified Communications Manager Administration, use the `System > LDAP > LDAP Custom Filter` menu path to configure LDAP filters.

In the LDAP Filter Configuration window, you specify information about the LDAP filter.

#### Before you begin

Before you can synchronize the LDAP directory, you must activate the Cisco DirSync service. For information about how to activate services, see the Cisco Unified Serviceability Administration Guide.

Changes to LDAP Directory information and LDAP Authentication settings are possible only if synchronization from the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

You can import and export LDAP custom filters by using the Bulk Administration Tool. For more information, see the Cisco Unified Communications Manager Bulk Administration Guide.
LDAP filter deletion

When you delete an LDAP filter, Cisco Unified Communications Manager removes that filter from the database.

You cannot delete an LDAP filter that is assigned to a directory agreement. To determine if an LDAP filter is assigned to a directory agreement, select Dependency Records from the Related Links drop-down list box in the LDAP Filter Configuration window. If any dependencies display for that LDAP filter, you cannot delete it.

LDAP filter settings

The following table describes the LDAP filter settings.

**Table 14: LDAP custom filter settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Custom Filter Information</td>
<td>Enter a name for the LDAP filter. The name can contain a maximum of 64 UTF-8 characters.</td>
</tr>
<tr>
<td>Filter Name</td>
<td>Enter a filter. The filter can contain a maximum of 1024 UTF-8 characters. Enclose the filter text within parentheses ().</td>
</tr>
<tr>
<td>Filter</td>
<td>The LDAP filter filters the results of LDAP searches. LDAP users that match the filter get imported into the Cisco Unified Communications Manager database, while LDAP users that do not match the filter do not get imported. The filter text that you enter must comply with the regular LDAP search filter standards specified in RFC 4515. It is recommended that you verify the LDAP search filter against the LDAP directory/searchbase by using the ldapssearch command. You apply LDAP filters to LDAP directories. For more information, see the LDAP directory setup, on page 93. You can apply an LDAP filter to multiple LDAP directories, and to all LDAP directory types for which the filter is valid.</td>
</tr>
</tbody>
</table>

Related Topics

- LDAP custom filter setup, on page 105
Location setup

This chapter provides information about using Cisco Unified Communications Manager Administration to configure location settings and resynchronizing location bandwidth.

- About location setup, page 107
- Location deletion, page 108
- Location settings, page 109
- Location Bandwidth Manager Group, page 113
- Location Bandwidth Manager Intercluster Replication Group Settings, page 114

About location setup

In Cisco Unified Communications Manager Administration, use the System > Location Info menu path to configure locations.

Use locations to implement call admission control in a centralized call-processing system. Call admission control 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 the locations. For more information, see topics related to call admission control in the Cisco Unified Communications Manager System Guide.

**Note**

If you do not use call admission control to limit the audio and video bandwidth on an IP WAN link, an unlimited number of calls can be active on that link at the same time. This situation can cause the audio quality of each audio call and the video quality of each video call to degrade as the link becomes oversubscribed.

**Tip**

Do not confuse locations with geolocations. Locations, which you configure by using the System > Location Info 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.
In a centralized call-processing system, a single Cisco Unified Communications Manager cluster provides call processing for all locations on the IP telephony network. The Cisco Unified Communications Manager cluster usually resides at the main (or central) location, along with other devices such as phones and gateways. The remote locations contain additional devices, but no Cisco Unified Communications Manager. IP WAN links connect the remote locations to the main location.

Cisco Unified Communications Manager supports up to 2000 locations. The following limitations and restrictions apply:

- Configure as many locations as possible to Use System Default for the RSVP policy.
- This enhancement requires an MCS 7845H1 or higher server.
- See the "Regions" subtopic under the "Administration Considerations" topic of the "IP Video Telephony" chapter of the Cisco Unified Communications Solution Reference Network Design (SRND) for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.

**Enhanced Location Call Admission Control**

The Enhanced Location Call Admission Control (CAC) feature improves the Location CAC mechanism to support more complex networks, including multi-tier, and multi-hop topologies. This feature supports Location CAC within a cluster and among multiple clusters, performing end to end bandwidth deduction. This enhancement to the CAC feature creates a much more flexible and dynamic system for the management of bandwidth.

The Enhanced Location CAC feature is provided by the Location Bandwidth Manager (LBM) service. The LBM service can be configured to run on every node or selected nodes of a Unified Communication Manager (Unified CM) server. For more information, see the chapter Enhanced Location Call Admission Control in the Cisco Unified Communications Manager Features and Services Guide.

**Related Topics**

- About Cisco Unified Communications Manager setup, on page 33
- CTI route point setup, on page 421
- Gateway setup, on page 433
- Cisco Unified IP Phone setup, on page 537

**Location deletion**

You cannot delete a location to which devices are assigned. To find out which devices are using the location, click Dependency Records from Related Links in the Location Configuration window; then, click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a location that is in use, Cisco Unified Communications Manager displays a message. Before deleting a location that is currently in use, you must perform either or both of the following tasks:

- Update the devices to assign them to a different location.
- Delete the devices that are assigned to the location that you want to delete.
Deleting a location allocates infinite bandwidth for the links that are connected to that location and allows an unlimited number of calls on those links. Deleting a location can cause audio quality on the links to degrade.

**Related Topics**

Access dependency records, on page 874

---

### Location settings

The following table describes the location settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the new location that you are creating. Three system locations are predefined:</td>
</tr>
<tr>
<td></td>
<td>• Hub_None—The Hub_None location specifies unlimited audio bandwidth and unlimited video bandwidth. A device that associates with the Hub_None location allows an unlimited number of active calls to or from the device. By default, devices not assigned to other locations are assigned to Hub_None.</td>
</tr>
<tr>
<td>Note</td>
<td>The location that is configured in a device pool takes precedence over the location configured in the device when the location in the device is set to Hub_None. If the device location is set to any other user-defined location, standard rules apply and the device parameter takes priority.</td>
</tr>
<tr>
<td></td>
<td>• Phantom—Phantom location specifies unlimited audio bandwidth, unlimited video bandwidth, and unlimited immersive video bandwidth. Specify this location to allow successful call admission control for calls across inter-cluster trunks that use the H.323 protocol or SIP trunks to certain destinations that support the earlier Location CAC feature.</td>
</tr>
<tr>
<td>Note</td>
<td>Both Hub_None and Phantom locations do allow configuration of the associated RSVP policy setting(s).</td>
</tr>
<tr>
<td></td>
<td>• Shadow—Shadow is a system location created for inter-cluster Enhanced Location CAC. In order to pass location information across clusters, the SIP ICT must be assigned to the system location Shadow.</td>
</tr>
</tbody>
</table>

| Links - Bandwidth Between This Location and Adjacent Locations |                                                                                                                                                                                                 |
| Select a location from the list.                           |                                                                                                                                                                                                 |
### Field Description

**Weight**
Enter the relative priority of this link in forming the Effective Path between any pair of Locations. The Effective Path has the least cumulative Weight of all possible paths. Valid values are 0-100.

**Audio Bandwidth**
Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link between this location and other locations. For audio calls, the audio bandwidth includes overhead. Choose between the following options:

- **Unlimited bandwidth**—Click the Unlimited radio button.
- **Specified bandwidth**—Specify a bandwidth by clicking the radio button next to the kb/s box and entering a specified bandwidth. Valid values are 1 to 2147483647.

For purposes of location bandwidth calculations only, assume that each call stream consumes the following amount of bandwidth:

- G.711 call uses 80 kb/s.
- G.722 call uses 80 kb/s.
- G.723 call uses 24 kb/s.
- G.728 call uses 16 kb/s.
- G.729 call uses 24 kb/s.
- GSM call uses 29 kb/s.
- Wideband call uses 272 kb/s.

**Note** To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed on this link.

### Video Calls Information

**Video Bandwidth**
Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Choose among the following options:

- **None**—The system does not allow video calls between this location and other locations.
- **Specified bandwidth**—Specify a video bandwidth by clicking the radio button next to the kb/s box and entering a specified video bandwidth. The default value specifies 384 kb/s.
- **Unlimited bandwidth**—Click the Unlimited radio button.

**Immersive Video Information**
**Field** | **Description**
---|---
Immersive Video | Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead. Choose among the following options:

- None—The system does not allow immersive video calls between this location and other locations. Immersive video calls can, however, take place within this location.
- Specified bandwidth—Specify an immersive video bandwidth by clicking the radio button next to the kb/s box and entering a specified immersive video bandwidth. The default value specifies 384 kb/s.
- Unlimited bandwidth—Click the Unlimited radio button.

Audio Bandwidth | Enter the maximum amount of audio bandwidth (in kb/s) that is available for all audio calls on the link within this location. For audio calls, the audio bandwidth includes overhead. Choose between the following options:

- Unlimited bandwidth—Click the Unlimited radio button.
- Specified bandwidth—Specify a bandwidth by clicking the radio button next to the kb/s box and entering a specified bandwidth. Valid values are 1 to 2147483647.

For purposes of location bandwidth calculations only, assume that each call stream consumes the following amount of bandwidth:

- G.711 call uses 80 kb/s.
- G.722 call uses 80 kb/s.
- G.723 call uses 24 kb/s.
- G.728 call uses 16 kb/s.
- G.729 call uses 24 kb/s.
- GSM call uses 29 kb/s.
- Wideband call uses 272 kb/s.

To improve audio quality, lower the bandwidth setting, so fewer active calls are allowed within this location.
### Field Description

**Video Bandwidth**  
Enter the maximum amount of video bandwidth (in kb/s) that is available for all video calls on the link between this location and other locations. For video calls, the video bandwidth does not include overhead. Choose among the following options:

- **None**—The system does not allow video calls between this location and other locations.
- **Specified bandwidth**—Specify a video bandwidth by clicking the radio button next to the kb/s box and entering a specified video bandwidth. The default value specifies 384 kb/s.
- **Unlimited bandwidth**—Click the Unlimited radio button.

### Immersive Video Information

**Immersive Video**  
Enter the maximum amount of immersive video bandwidth (in kb/s) that is available for all immersive video calls on the link within this location. For video calls, the immersive video bandwidth does not include overhead. Choose among the following options:

- **None**—The system does not allow immersive video calls between this location and other locations. Immersive video calls can, however, take place within this location.
- **Specified bandwidth**—Specify an immersive video bandwidth by clicking the radio button next to the kb/s box and entering a specified immersive video bandwidth. The default value specifies 384 kb/s.
- **Unlimited bandwidth**—Click the Unlimited radio button.

### Locations RSVP Settings

**Location**  
This display-only field displays locations for which the inter-location RSVP setting has been changed from the system default RSVP policy.

**RSVP Setting**  
This display-only field displays the RSVP policy setting between the selected location and the location that is listed in the Location column to the left.

### Modify Setting(s) to Other Locations

**Location**  
To change the RSVP policy setting between the current location and a location that displays in this pane, choose a location in this pane.
To choose an RSVP policy setting between the current location and the location that is chosen in the Location pane at left, choose an RSVP setting from the drop-down list box. Choose from the following available settings:

- **Use System Default**—The RSVP policy for the location pair matches the clusterwide RSVP policy. See topics related to clusterwide default RSVP policy in the Cisco Unified Communications Manager System Guide for details.

- **No Reservation**—No RSVP reservations can get made between any two locations.

- **Optional (Video Desired)**—A call can proceed as a best-effort audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP Agent continues to attempt RSVP reservation and informs Cisco Unified Communications Manager if reservation succeeds.

- **Mandatory**—Cisco Unified Communications Manager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well.

- **Mandatory (Video Desired)**—A video call can proceed as an audio-only call if a reservation for the video stream cannot be reserved.

---

**Location Bandwidth Manager Group**

In Cisco Unified Communications Manager Administration, use the System > Location Info > Location Bandwidth Manager Group menu path to configure which Location Bandwidth Manager (LBM) services each Cisco Callmanager service communicate with.

Each Cisco Callmanager service must communicate with an LBM service to determine the availability of bandwidth for each call, and to deduct bandwidth for the duration of each call that is admitted.

The LBM Group Page allows the Cisco Callmanager service to communicate with selected LBM services, instead of communicating with the local LBM service.

**Table 16: Location Bandwidth Manager Group Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Bandwidth Manager Group Setting</td>
<td>To choose an RSVP policy setting between the current location and the location that is chosen in the Location pane at left, choose an RSVP setting from the drop-down list box. Choose from the following available settings:</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the new Location Bandwidth Manager Group that you are creating.</td>
</tr>
<tr>
<td>Description</td>
<td>If desired enter a description for the Location Bandwidth Manager Group.</td>
</tr>
<tr>
<td>Location Bandwidth Manager Group Members</td>
<td>If desired enter a description for the Location Bandwidth Manager Group.</td>
</tr>
<tr>
<td>Active Member</td>
<td>Select the active member from the list.</td>
</tr>
</tbody>
</table>
If desired select a standby LBM to be used when the active LBM is not reachable.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standby Member</td>
<td>If desired select a standby LBM to be used when the active LBM is not reachable.</td>
</tr>
</tbody>
</table>

**Location Bandwidth Manager Intercluster Replication Group Settings**

In Cisco Unified Communications Manager Administration, use the **System > Location Info > Location Bandwidth Manager (LBM) Intercluster Replication Group** menu path to configure LBM Intercluster Replication Group.

LBM Intercluster Replication Group configuration enables an LBM service to participate either directly or indirectly in intercluster replication of configured and dynamic Location Bandwidth data. LBMs assigned an LBM hub role participate directory in intercluster replication of Location Bandwidth data. LBM hubs discover each other through their common connections and form a fully-meshed replication network. LBMs assigned a spoke role participate indirectly in intercluster replication through the LBM hubs in their cluster.

Use the LBM Intercluster Replication Group Page to configure the LBM Intercluster Replication service to find a location in the remote clusters to establish external communication.

**Table 17: LBM Intercluster Replication Group Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Information</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the new LBM Intercluster Replication Group that you are creating.</td>
</tr>
<tr>
<td>Description</td>
<td>If desired enter a description for the LBM Intercluster Replication Group.</td>
</tr>
<tr>
<td>Bootstrap Servers</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>Add servers to the list.</td>
</tr>
<tr>
<td>Role Assignment</td>
<td></td>
</tr>
<tr>
<td>LBM Services</td>
<td>Services in this list become LBM hubs.</td>
</tr>
<tr>
<td>Assigned to Hub Role</td>
<td></td>
</tr>
<tr>
<td>LBM Services not</td>
<td>Services in this list become LBM spokes.</td>
</tr>
<tr>
<td>Assigned to Hub Role</td>
<td></td>
</tr>
</tbody>
</table>
Survivable remote site telephony setup

This chapter provides information to add, update, copy, or delete a SRST reference. For additional information, see topics related to survivable remote site telephony references in the *Cisco Unified Communications Manager System Guide*.

- About SRST reference setup, page 115
- SRST reference deletion, page 115
- SRST reference settings, page 116

### About SRST reference setup

In Cisco Unified Communications Manager Administration, use the **System > SRST** menu path to configure SRST references.

A survivable remote site telephony (SRST) reference comprises the gateway that can provide limited Cisco Unified Communications Manager functionality when all other Cisco Unified Communications Manager servers for a device are unreachable. Typically assigned to device pools, SRST references determine the gateways where calling devices search when they attempt to complete a call if Cisco Unified Communications Manager is unavailable. For more detailed information on SRST references, see topics related to SRST reference configuration settings in the *Cisco Unified Communications Manager System Guide*.

### SRST reference deletion

You cannot delete SRST references that device pools or other items are using. To find out which device pools are using the SRST reference, click the Dependency Records link from the SRST Reference Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete an SRST reference that is in use, Cisco Unified Communications Manager displays an error message. Before deleting an SRST reference that is currently in use, you must perform either or both of the following tasks:

- Assign a different SRST reference to any device pools that are using the SRST reference that you want to delete.
- Delete the device pools that are using the SRST reference that you want to delete.
Before initiating a deletion, check carefully to ensure that you are deleting the correct SRST reference. You cannot retrieve deleted SRST references. If an SRST reference is accidentally deleted, you must rebuild it.

Related Topics
- About device pool setup, on page 63
- Access dependency records, on page 874

SRST reference settings

The following table describes the SRST reference settings.

**Table 18: SRST reference settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name in the SRST Reference Name field. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each SRST reference name is unique.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Use concise and descriptive names for your SRST references.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number for this SRST reference. Default value specifies 2000.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Change this value only if it does not match the gateway port setting.</td>
</tr>
<tr>
<td></td>
<td>This value and the gateway port setting must match.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the gateway for devices in a device pool to use as an SRST reference.</td>
</tr>
<tr>
<td>SIP Network/IP Address</td>
<td>Enter the IP address of the server that the phones that are running SIP will use when in SRST mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> You must configure the SIP Network/IP Address field and the SIP Port field for a SIP device to fall back to the SRST-enabled gateway.</td>
</tr>
<tr>
<td>SIP Port</td>
<td>Enter the SIP port of the SRST gateway. Default value specifies 5060.</td>
</tr>
<tr>
<td>Is SRST Secure?</td>
<td>After you verify that the SRST-enabled gateway contains a self-signed certificate, check this check box.</td>
</tr>
<tr>
<td></td>
<td>After you configure the SRST and reset the gateway and dependent phones, the Cisco CTL Provider service authenticates to the Certificate Provider service on the SRST-enabled gateway. The Cisco CTL client retrieves the certificate from the SRST-enabled gateway and stores the certificate in the Cisco Unified Communications Manager database.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> To remove the SRST certificate from the database and phone, uncheck this check box, click Save, and reset the dependent phones.</td>
</tr>
</tbody>
</table>
This port monitors requests for the Certificate Provider service on the SRST-enabled gateway. Cisco Unified Communications Manager uses this port to retrieve the certificate from the SRST-enabled gateway. The Cisco SRST Certificate Provider default port equals 2445.

After you configure this port on the SRST-enabled gateway, enter the port number in this field.

**Tip**  
You may need to configure a different port number if the port is currently used or if you use a firewall and you cannot use the port within the firewall.

**Update Certificate**

**Tip**  
This button displays only after you check the Is SRST Secure? check box and click Save. After you click this button, the Cisco CTL client replaces the existing SRST-enabled gateway certificate that is stored in the Cisco Unified Communications Manager database, if a certificate exists in the database. After you reset the dependent phones, the TFTP server sends the cnf.xml file (with the new SRST-enabled gateway certificate) to the phones.

**Related Topics**

- Survivable remote site telephony setup, on page 115
CHAPTER 17

MLPP Domain setup

This chapter provides information to add, update, or delete MLPP domains.

For additional information, see topics related to multilevel precedence and preemption in the *Cisco Unified Communications Manager Features and Services Guide*.

- About MLPP Domain Setup, page 119
- MLPP domain deletion, page 119
- MLPP domain settings, page 120

About MLPP Domain Setup

In Cisco Unified Communications Manager Administration, use the **System > MLPP > Domain > MLPP Domain** menu path to configure MLPP domains.

An MLPP domain 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.

**MLPP domain configuration tips**

You can add secure MLPP over SIP trunks by configuring a Resource Priority Namespace Network Domain and Resource Priority Namespace List.

**Related Topics**

- About Resource Priority Namespace Network Domain setup, on page 121
- About Resource Priority Namespace List setup, on page 123

MLPP domain deletion

You cannot delete an MLPP Domain that any device is using. To find out which devices are using the MLPP domain, from the MLPP Domain Configuration window, choose Dependency Records from the Related Links drop-down list box 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 *Access
dependency records, on page 874. If you try to delete an MLPP Domain that is in use, Cisco Unified Communications Manager displays an error message. Before deleting an MLPP Domain that is currently in use, you must perform either or both of the following tasks:

• Assign a different MLPP domain to any devices that are using the MLPP domain that you want to delete.
• Delete the devices that are using the MLPP domain that you want to delete.

MLPP domain settings

The following table describes the MLPP domain settings.

Table 19: MLPP domain settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Domain Information</td>
<td></td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the name that you want to assign to the new MLPP domain. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each MLPP domain name is unique.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The name of the default MLPP domain specifies 000000. The Default domain cannot be changed nor deleted.</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Enter a unique six-character hexadecimal MLPP domain ID. Valid values are numeric characters 0 through 9 and alphabetic characters A through F. Ensure that each MLPP domain ID is unique. Domain IDs must fall in the range between 000001 and FFFFFFF. (000000 is reserved for the default MLPP domain ID.)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Use leading zeroes for values lower than 100000.</td>
</tr>
</tbody>
</table>

Related Topics

MLPP Domain setup, on page 119
Resource Priority Namespace Network Domain setup

This chapter provides information to add, update, or delete Resource Priority Namespace Network Domains. For additional information, see topics related to multilevel precedence and preemption in the Cisco Unified Communications Manager Features and Services Guide.

- About Resource Priority Namespace Network Domain setup, page 121
- Resource Priority Namespace Network Domain deletion, page 122
- Resource Priority Namespace Network Domain settings, page 122

About Resource Priority Namespace Network Domain setup

In Cisco Unified Communications Manager Administration, use the System > MLPP > Namespace > Resource Priority Namespace Network Domain menu path to configure Resource Priority Namespace Network Domains.

Cisco Unified Communications Manager uses Resource Priority Namespace Network Domains to support Voice over Secured IP (VoSIP) networks by using Multilevel Precedence and Preemption (MLPP) for Session Initiation Protocol (SIP) trunks.

MLPP, with configured Resource Priority domains, prioritizes SIP–signaled resources and enables indications related to precedence and preempted calls. End users can establish secure calls when the calls traverse SIP trunks.

There are five registered namespaces for resource priority:

1. dsn—Defense Switched Network
2. drsn—Defense Red Switched Network
3. q735—Commercial equivalent of the DSN
4. ets—Emergency Telephone Service
5. wps—Wireless Priority Service
Cisco Unified Communications Manager accepts "Q735" and "q735" as the same value. It transmits "q735" when signaling an MLPP call on the SIP trunk.

Resource Priority Namespace Network Domain deletion

You cannot delete a Resource Priority Namespace Network Domain that any device is using. To find out which devices are using the Resource Priority Namespace Network Domain, from the Resource Priority Namespace Network Domain Configuration window, choose Dependency Records from the Related Links drop-down list box 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.

If you try to delete a Resource Priority Namespace Network Domain that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a Resource Priority Namespace Network Domain that is currently in use, you must perform either or both of the following tasks:

- Assign a different Resource Priority Namespace Network Domain to any devices that are using the Resource Priority Namespace Network Domain that you want to delete.
- Delete the devices that are using the Resource Priority Namespace Network Domain that you want to delete.

Related Topics

Access dependency records, on page 874

Resource Priority Namespace Network Domain settings

The following table describes the Resource Priority Namespace Network Domain settings.

Table 20: Resource Priority Namespace Network Domain settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the Resource Priority Namespace Network Domain in the information section. The maximum number of domain names is 100.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the domain name. 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>
<tr>
<td>Make this the Default Resource Priority Namespace Network Domain</td>
<td>Check the box if you want the domain name to be the default.</td>
</tr>
</tbody>
</table>

Related Topics

Resource Priority Namespace Network Domain setup, on page 121
CHAPTER 19

Resource Priority Namespace List setup

This chapter provides information to add, update, or delete Resource Priority Namespace Lists.

- About Resource Priority Namespace List setup, page 123
- Resource Priority Namespace List deletion, page 123
- Resource Priority Namespace List settings, page 124

About Resource Priority Namespace List setup

In Cisco Unified Communications Manager Administration, use the System > MLPP > Namespace > Resource Priority Namespace List menu path to configure Resource Priority Namespace Lists.

Cisco Unified Communications Manager uses Resource Priority Namespace Lists to configure a default group of Resource Priority Namespace Network Domains to add to a SIP profile for validating incoming Resource Priority Namespace Network Domains.

Resource Priority Namespace List deletion

You cannot delete a Resource Priority Namespace List that any device is using. To find out which devices are using the Resource Priority Namespace List, from the Resource Priority Namespace List Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete an Resource Priority Namespace List that is in use, Cisco Unified Communications Manager displays an error message. Before deleting an Resource Priority Namespace List that is currently in use, you must perform either or both of the following tasks:

- Assign a different Resource Priority Namespace List to any devices that are using the Resource Priority Namespace List that you want to delete.
- Delete the devices that are using the Resource Priority Namespace List that you want to delete.

Related Topics

Access dependency records, on page 874
Resource Priority Namespace List settings

The following table describes the Resource Priority Namespace List settings.

Table 21: Resource priority namespace list settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the Resource Priority Namespace List. The maximum number of characters is 50.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the list. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Available Resource Priority Namespaces</td>
<td>Use the Up and Down Arrows to select or deselect already configured Resource Priority Namespace Network Domains.</td>
</tr>
<tr>
<td>Selected Resource Priority Namespaces</td>
<td>Displays the selected Resource Priority Namespace Network Domains.</td>
</tr>
</tbody>
</table>

Related Topics

Resource Priority Namespace List setup, on page 123
E911 messages

Users of devices designated for off-premises use are first presented with various messages, which assure that users are aware of the need to provide correct location information.

The E911 Messages page allows you to view and edit the messages that can be displayed on an off-premise device. The Find-List for these messages is different than the traditional Find-List. Instead of listing individual messages, the list is shown as message sets based on the language, for example English, American. Selecting a language takes you to the page where you can edit and save the messages.

- E911 messages setup, page 125
- Set up E911 Messages, page 125

E911 messages setup

Users of devices designated for off-premises use are first presented with various messages, which assure that users are aware of the need to provide correct location information.

The E911 Messages page allows you to view and edit the messages that can be displayed on an off-premise device. The Find-List for these messages is different than the traditional Find-List. Instead of listing individual messages, the list is shown as message sets based on the language, for example English, American. Selecting a language takes you to the page where you can edit and save the messages.

Set up E911 Messages

Use the following procedure to select and edit E911 messages for off-premises devices using Unified CM.

Procedure

**Step 1** Choose System > E911 Messages.

**Step 2** Select the required language link of the E911 messages.

The E911 Messages Configuration page displays the Agreement, Disclaimer, and Error messages.
Step 3  Optionally, you can edit the E911 messages to be displayed on off-premises devices.
Step 4  Click Save.
CHAPTER 21

Enterprise parameter setup

This chapter provides information to update existing enterprise parameters or synchronize enterprise-parameter configuration changes with affected devices.

- About enterprise parameter setup, page 127
- Update enterprise parameters, page 128
- Synchronize enterprise parameters with devices, page 128

About enterprise parameter setup

Enterprise parameters provide default settings that apply to all devices and services in the same cluster. (A cluster comprises a set of Cisco Unified Communications Managers that share the same database.) When you install a new Cisco Unified Communications Manager, it uses the enterprise parameters to set the initial values of its device defaults. For more information on device defaults, see topics related to system-level configuration settings in the Cisco Unified Communications Manager System Guide.

Note

Many of the enterprise parameters rarely require change. Do not change an enterprise parameter unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the change.

Tip

To view the descriptions of all enterprise parameters, click the ? button in the Enterprise Parameters Configuration window.

Tip

Clicking the Set to Default button updates all parameters to the suggested value, which is the default that displays on the right side of the parameter. If a parameter does not have a suggested value, Cisco Unified Communications Manager does not update the value when you click the Set to Default button; for example, the Phone URL Parameters in the Enterprise Parameters Configuration window do not display a suggested value, so clicking the Set to Default button does not change the value that you configured.
Update enterprise parameters

Procedure

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

**Step 2** Update the appropriate parameter settings.
To view the description of a particular enterprise parameter, click the parameter name. To view the descriptions of all the enterprise parameters, click the ? button.

**Step 3** To save the changes in the database, click Save.

Synchronize enterprise parameters with devices

To synchronize devices with Enterprise Parameters that have undergone configuration changes, perform the following procedure, which applies 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 System > Enterprise Parameters.
The Enterprise Parameters Configuration window displays.

**Step 2** Make any necessary configuration changes.

**Step 3** Click Save.

**Step 4** Click Apply Config.
The Apply Configuration Information dialog displays.

**Step 5** Click OK.
Enterprise phone setup

This chapter provides information to configure the Enterprise Phone parameters. In the Enterprise Phone Configuration window, you can configure parameters that apply to all phones that support these parameters.

- Set up enterprise phone parameters, page 129

Set up enterprise phone parameters

To configure parameters in the Enterprise Phone Configuration window, use the following procedure.

**Procedure**

**Step 1** Choose System > Enterprise Phone Configuration.

**Step 2** Update the parameter settings as desired. Select the "Override Common Settings" check box for each setting that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect.

To view the descriptions of all the enterprise phone parameters, click the ? button.

**Step 3** To save the changes in the database, click Save.

**Note** Parameters that you set in this window may also appear in the Common Phone Profile Configuration window and in the Phone Configuration window for various devices. If you set these same parameters in these other windows too, the following order determines the setting that takes precedence: 1) Phone Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.
Set up enterprise phone parameters
Service parameter setup

This chapter provides information to configure and display different services on selected servers using Cisco Unified Communications Manager. You can view a list of service parameters and their descriptions by clicking the ? icon in the Service Parameter Configuration window.

For information about what happens to service parameter values during an upgrade, see Upgrading Cisco Unified Communications Manager.

For more information about Cisco Unified Communications Manager services, see the Cisco Unified Serviceability Administration Guide.

• About server service parameter setup, page 131
• Set up server service parameters, page 133
• Display service parameters, page 133

About server service parameter setup

In Cisco Unified Communications Manager Administration, use the System > Service Parameters menu path to configure service parameters.

Service parameters for Cisco Unified Communications Manager allow you to configure different services on selected servers. You can view a list of parameters and their descriptions by clicking the ? icon in the Service Parameter Configuration window.

If you deactivate a service by using Cisco Unified Serviceability, Cisco Unified Communications Manager retains any updated service parameter values. If you start the service again, Cisco Unified Communications Manager sets the service parameters to the changed values.

Consider the following information before you configure the service parameters in the Service Parameters Configuration window:

• For information about what happens to service parameter values during an upgrade, see Upgrading Cisco Unified Communications Manager.
To configure service parameters, you must select a single server and a single service on that server. After you make the selection you can configure parameters for the service on that single serve and on others that apply to the service on all servers within the cluster; these get marked as clusterwide. Unlike enterprise parameters that apply to all services, each service gets configured with a separate set of service parameters.

Feature services, which display under Service Activation and Control Center–Feature Services in Cisco Unified Serviceability, can display as active or inactive in the Service Parameters Configuration window. If you activated the feature service in Cisco Unified Serviceability, the service displays as active in the Service Parameters Configuration window; for example, Cisco CallManager (active). If you have not activated the feature service, the service displays as inactive in the Service Parameters Configuration window.

Network services, which display under Control Center–Network Services in Cisco Unified Serviceability, always display as active in the Service Parameters Configuration window; for example, Cisco DRF Master (active). With network services, you do not need to start the service in Cisco Unified Serviceability because it automatically runs on the server after the Cisco Unified Communications Manager installation/upgrade.

In the Service Parameters Configuration window, be aware that network services display as active even for dummy nodes, which are servers that display in the Server Configuration window in Cisco Unified Communications Manager Administration but that do not have Cisco Unified Communications Manager installed on them.

For more information about Cisco Unified Communications Manager services, see the Cisco Unified Serviceability Administration Guide.

In the Server drop-down list box in the Service Parameter Configuration window, all servers, including dummy nodes, display as active; for example, <servername> (active). In this case, active means that you provisioned the server in Cisco Unified Communications Manager Administration.

If you deactivate a service by using Cisco Unified Serviceability, Cisco Unified Communications Manager retains any updated service parameter values. If you start the service again, Cisco Unified Communications Manager sets the service parameters to the changed values.

Clicking the Set to Default button updates all parameters to the suggested value, which is the default that displays on the right side of the parameter. If a parameter does not have a suggested value, Cisco Unified Communications Manager does not update the value when you click the Set to Default button; for example, the Mobile Voice Access service parameter for the Cisco CallManager service does not display a suggested value, so clicking the Set to Default button does not change the value that you enter for this parameter.

Some changes to service parameters may cause system failure. Cisco recommends that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) specifies the changes.

You can configure a SIP trunk to use a DNS SRV port on a Cisco Unified Presence server as a destination. If you use a SIP trunk with a DNS SRV destination to configure the CUP Publish Trunk service parameter and then modify the DNS record, you must restart all devices (phones) that previously published, so they point to the correct Cisco Unified Presence server destination.
Set up server service parameters

You can configure the service parameters for a particular service on a particular server.

**Before You Begin**

Ensure the following prerequisites are met before proceeding with the steps:

- Make sure that servers are configured.
- Make sure that the service is available on the servers. The Service Parameter Configuration window displays all the available services. For more information on services, see the *Cisco Unified Serviceability Administration Guide* for more information.

**Procedure**

1. **Step 1** Choose **System > Service Parameters**.
2. **Step 2** From the Server drop-down list box, choose a server.
3. **Step 3** From the Service drop-down list box, choose the service that contains the parameter that you want to update. **Note** The Service Parameter Configuration window displays all services (active or not active).
4. **Step 4** Update the appropriate parameter value. To set all service parameters for this instance of the service to the default values, click the Set to Default button. To view a list of parameters and their descriptions, click the ? icon. To view the list with a particular parameter at the top, click that parameter in the Service Parameter Configuration window. **Note** Some services contain service parameters that should rarely be changed. Cisco Unified Communications Manager Administration does not automatically display these parameters when you access the Service Parameter Configuration window. To view all parameters, click Advanced. After all parameters display, you can redisplay the basic parameters by clicking Condensed. If the Advanced button is disabled, all parameters for that service display by default.
5. **Step 5** Click Save. The window refreshes, and Cisco Unified Communications Manager updates the service parameter with your changes.

**Related Topics**

- Server setup, on page 25
- About server service parameter setup, on page 131

Display service parameters

You may need to compare all service parameters that belong to a particular service on all servers in a cluster. You may also need to display only out-of-sync parameters (that is, service parameters for which values differ from one server to another) or parameters that have been modified from the suggested value.
Use the following procedure to display the service parameters for a particular service on all servers in a cluster.

**Procedure**

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

**Step 2** From the Server drop-down list box, choose a server.

**Step 3** From the Service drop-down list box, choose the service for which you want to display the service parameters on all servers in a cluster.

**Note** The Service Parameter Configuration window displays all services (active or not active).

**Step 4** In the Service Parameter Configuration window that displays, choose Parameters for All Servers in the Related Links Drop-down List Box; then, click Go.

The Parameters for All Servers window displays. For the current service, the list shows all parameters in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click on the server name or on the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Parameters for All Servers windows.

**Step 5** If you need to display out-of-sync service parameters, choose Out of Sync Parameters for All Servers in the Related Links drop-down list box, then click Go.

The Out of Sync Parameters for All Servers window displays. For the current service, service parameters that have different values on different servers display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click the server name or the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Out of Sync Parameters for All Servers windows.

**Step 6** If you need to display service parameters that have been modified from the suggested value, choose Modified Parameters for All Servers in the Related Links drop-down list box; then, click Go.

The Modified Parameters for All Servers window displays. For the current service, service parameters that have values that differ from the suggested values display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that have different values from the suggested values displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click the server name or the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Modified Parameters for All Servers windows.
Application server setup

This chapter provides information about working with and configuring application servers in Cisco Unified Communications Manager Administration.

For additional information, see topics related to Cisco Unity messaging integration in the Cisco Unified Communications Manager System Guide.

- About application server setup, page 135
- Application server settings, page 136

About application server setup

In Cisco Unified Communications Manager Administration, use the System > Application Server menu path to configure application servers.

You can use the Application Server windows in Cisco Unified Communications Manager Administration to maintain associations between the Cisco Unified Communications Manager and off-cluster, external applications, such as Cisco Unity Connection, Cisco Unified CM IM and Presence, and Cisco Emergency Responder, and to synchronize Cisco Unified Communications Manager systems and applications, such as Cisco Web Dialer.

Tip

Application server configuration does not support Cisco Unity Connection 2.x. To push a list of valid user templates for Cisco Unity Connection 2.x to Cisco Unified Communications Manager, create an AXL connection via Cisco Unity Connection 2.x, as described in the System Administration Guide for Cisco Unity Connection.

Application server configuration tips

You can configure the application servers in Cisco Unified Communications Manager Administration after both the Cisco Unified Communications Manager servers and any other application servers are set up and fully operational and are running with a valid configuration.
For Cisco Unity and Cisco Unity Connection, make sure that AXL is running on the Cisco Unified Communications Manager server that was configured to communicate with the Cisco Unity and Cisco Unity Connection server.

**Application server settings**

The following table describes all the available settings in the Application Server window. Because each server requires different settings, not all the settings in the table below apply to each server.

**Table 22: Application server settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server Information</td>
<td></td>
</tr>
<tr>
<td>Application Server Type</td>
<td>Choose the applicable application server for the type of application to which you want to connect (for example, to connect to a presence application server, choose Cisco Unified CM IM and Presence).</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify the application server that you are configuring.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the server that you are configuring. <strong>Note</strong> Ensure the IP address is numeric with a number pattern between 1-255 (10.255.172.57). <strong>Tip</strong> For Cisco Unity and Cisco Unity Connection, you must use the same Administrator user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration. This user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td>URL</td>
<td>Enter a URL for the application server.</td>
</tr>
<tr>
<td>End User URL</td>
<td>Enter a URL for the end users that are associated with this application server.</td>
</tr>
<tr>
<td>Available Application Users</td>
<td>This pane displays the application users that are available for association with this application server. To associate an application user with this application server, select the application user (for example, CCMAdmimistrator, CCMSysUser, UnityConnection, and so on) and click the Down arrow below this pane.</td>
</tr>
<tr>
<td>Selected Application Users</td>
<td>This pane displays the application users that are associated with the application server. To remove an application user, select the application user and click the Up arrow above this pane. To add an application user, select an application user in the Available Application Users pane and click the Down arrow.</td>
</tr>
</tbody>
</table>
Related Topics

Application server setup, on page 135
Application server settings
Autoregistration setup

This chapter provides information to configure, enable, and disable autoregistration, as well as information to reuse autoregistration numbers.

• About autoregistration setup, page 139
• Autoregistration settings, page 139
• Enable autoregistration, page 141
• Disable autoregistration, page 143
• Reuse autoregistration numbers, page 143

About autoregistration setup

Use autoregistration if you want Cisco Unified Communications Manager to assign directory numbers automatically to new phones as they connect to the Cisco Unified Communications IP telephony network.

Note

Cisco recommends that you use autoregistration to add fewer than 100 phones to your network. To add more than 100 phones to your network, use the Bulk Administration Tool (BAT).

After a phone has autoregistered, you can move it to a new location and assign it to a different device pool without affecting its directory number.

Autoregistration settings

The following table describes the autoregistration settings.
Table 23: Autoregistration settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Directory Number</td>
<td>Enter the first directory number to use for autoregistration of devices. Specifying a range of directory numbers in the Starting Directory Number and Ending Directory Number fields automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.</td>
</tr>
<tr>
<td>Ending Directory Number</td>
<td>Enter the last directory number to use for autoregistration of devices. The Ending Directory Number must be greater than the Starting Directory Number which automatically enables autoregistration. Setting the starting and ending directory numbers to the same value disables autoregistration.</td>
</tr>
<tr>
<td>Partition</td>
<td>Choose the partition to which autoregistered directory numbers belong. If you are not using partitions, choose &lt;None&gt;. You must choose a valid directory number range for autoregistration before you can choose a partition and external phone number mask. The partition field resets if you disable autoregistration. If a large number of partitions exist, the Find button displays next to the drop-down list box. Click the Find button to display the Find and List Partitions window. In the Find partition where field, choose search criteria and enter a partial partition name. In the list of partitions that displays, click the desired partition name and click OK.</td>
</tr>
<tr>
<td>External Phone Number Mask</td>
<td>Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the autoregistered devices. The mask can contain up to 50 characters. Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the autoregistered device. For example, if you specify a mask of 972813XXXX and enable the Use External Phone Number Mask option on the route pattern that is used to make the external call, an external call from extension 1234 displays a caller ID number of 9728131234. If you specify a mask of all literal digits (such as 9728135000) to represent a main attendant number, that literal number becomes the caller ID that displays for an external call from any autoregistered device.</td>
</tr>
</tbody>
</table>
Enable autoregistration

This section describes how to enable autoregistration for new devices.

Caution

Cisco Unified Communications Manager disables autoregistration by default. Enabling autoregistration carries a security risk in that "rogue" phones can automatically register with Cisco Unified Communications Manager. You should enable autoregistration only for brief periods when you want to perform bulk phone adds.

Configuring mixed mode clusterwide security through the Cisco CTL Client automatically disables autoregistration. If you want to use autoregistration and you have configured security, you must change the clusterwide security mode to non-secure through the Cisco CTL Client.

Before You Begin

Check the following points before you begin to enable autoregistration:

• Ensure that the TFTP server is up and running. Ensure that the DHCP option for TFTP specifies the correct server.
• Check that the Device Defaults Configuration window specifies the correct phone image names for SIP and SCCP. Ensure that these files are available on the TFTP server.
• Ensure that directory numbers are available in the autoregistration range.
• Ensure enough license points are available to register new phones.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-registration Disabled on this Cisco Unified Communications Manager</td>
<td>Cisco Unified Communications Manager disables autoregistration by default to prevent unauthorized connections to the network. When autoregistration is disabled, you must configure the directory numbers manually whenever you add new devices to your network.</td>
</tr>
<tr>
<td>• Uncheck the Auto-registration Disabled option to enable autoregistration for this Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>• Check the Auto-registration Disabled option to disable autoregistration for this Cisco Unified Communications Manager.</td>
<td></td>
</tr>
<tr>
<td>You can disable autoregistration by setting the Starting Directory Number and Ending Directory Number to the same value.</td>
<td></td>
</tr>
<tr>
<td>If starting and ending directory numbers are specified when you disable autoregistration by checking this option, Cisco Unified Communications Manager sets the starting and ending directory numbers to the same value.</td>
<td></td>
</tr>
<tr>
<td>The partition and external phone mask information fields also reset when you disable autoregistration.</td>
<td></td>
</tr>
</tbody>
</table>
**Procedure**

**Step 1** Choose System > Enterprise Parameters. The Enterprise Parameters Configuration window displays.

**Step 2** In the Auto Registration Phone Protocol drop-down list box, choose either SCCP or SIP.

**Step 3** Choose System > Cisco Unified CM. The Find and List Cisco Unified Communications Managers window displays. Click Find.

**Step 4** From the list of Cisco Unified Communications Managers, choose the Cisco Unified Communications Manager, in the cluster, that you want to enable for autoregistration.

**Note** Always enable or disable autoregistration only on this Cisco Unified Communications Manager. If you shift the autoregistration function to another Cisco Unified Communications Manager in the cluster, you must reconfigure the appropriate Cisco Unified Communications Managers, the Default Cisco Unified Communications Manager Group, and, possibly, the default device pools.

**Step 5** Enter the appropriate Autoregistration Information, as described in Table 23: Autoregistration settings, on page 140.

**Step 6** To save the changes in the database, click Save.

**Step 7** Choose System > Cisco Unified CM Group. The Find and List Cisco Unified Communications Manager Groups window displays.

**Step 8** Click Find.

**Step 9** From the list of Cisco Unified Communications Manager groups, choose the group that is enabled for autoregistration. (In most systems, the name of this group specifies Default. You can, however, choose a different Cisco Unified Communications Manager group.) This group serves as the default Cisco Unified Communications Manager group for devices that autoregister. Ensure that the Selected Cisco Unified Communications Managers list for this group contains the Cisco Unified Communications Manager that you configured for autoregistration in Enable autoregistration, on page 141. The Cisco Unified Communications Managers get selected in the order in which they are listed in the Cisco Unified Communications Manager group.

**Step 10** If you made any changes to the group configuration, click Save to save the changes in the database.

**Step 11** Configure a calling search space specifically for autoregistration. For example, you can use the autoregistration calling search space to limit autoregistered phones to internal calls only.

**Step 12** Configure the Default device pool for autoregistration by assigning the Default Cisco Unified Communications Manager Group and autoregistration calling search space to the Default device pool. If you are configuring a separate default device pool for each device type, use the Device Defaults Configuration window to assign the default device pools to the device.

**Step 13** Enable autoregistration only during brief periods when you want to install and autoregister new devices (preferably when overall system usage is at a minimum). During other periods, turn autoregistration off to prevent unauthorized devices from registering with Cisco Unified Communications Manager.

**Step 14** Install the devices that you want to autoregister.

**Step 15** Reconfigure the autoregistered devices and assign them to their permanent device pools.

**Step 16** In the Enterprise Parameters Configuration window, set the Auto Registration Phone Protocol setting to SIP or SCCP, whichever is needed.

**Step 17** If you autoregister more phones with a different protocol, repeat Step 1, on page 142 through Step 16, on page 142.
Disable autoregistration

This section describes how to disable autoregistration.

Procedure

Step 1  Choose System > Cisco Unified CM.
Step 2  From the Cisco Unified Communications Manager list, choose the Cisco Unified Communications Manager where you want to disable autoregistration.
Step 3  To disable autoregistration for this Cisco Unified Communications Manager, click the Auto-registration Disabled on this Cisco Unified Communications Manager checkbox. (When this box is checked, autoregistration specifies disabled.)

Note  You can also disable autoregistration by setting the Starting Directory Number and Ending Directory Number to the same value.

Step 4  To save the changes in the database, click Save.
Step 5  Repeat Step 2, on page 143 through Step 4, on page 143 for each Cisco Unified Communications Manager where you want to disable autoregistration.

Reuse autoregistration numbers

When you connect a new device to the network, Cisco Unified Communications Manager assigns the next available (unused) autoregistration directory number to that device. If you manually change the directory number of an autoregistered device, or if you delete that device from the database, Cisco Unified Communications Manager can reuse the autoregistration directory number of that device.

When a device attempts to autoregister, Cisco Unified Communications Manager searches the range of autoregistration numbers that you specified and tries to find the next available directory number to assign to the device. It begins the search with the next directory number in sequence after the last one that was assigned. If it reaches the ending directory number in the range, Cisco Unified Communications Manager continues to search from the starting directory number in the range.

You can use the following procedure to reset the range of autoregistration directory numbers and force Cisco Unified Communications Manager to search from the starting number in the range.
Procedure

**Step 1** Choose **System > Cisco Unified Communications Manager**.

**Step 2** Choose the Cisco Unified Communications Manager where you want to reset autoregistration.

**Step 3** Write down the current settings for Starting Directory Number and Ending Directory Number.

**Step 4** Click Auto-registration Disabled on this Cisco Unified Communications Manager.

**Caution** New phones cannot autoregister while autoregistration is disabled.

**Step 5** Click Save.

**Step 6** Set the Starting Directory Number and Ending Directory Number to their previous values (or to new values, if desired).

**Step 7** Click Save.

**Related Topics**

Autoregistration setup, on page 139
Other system menu options

This chapter provides brief descriptions of selected System menu options. A pointer to documents that contain a more detailed description for each of these System menu options is provided.

- BLF presence group setup, page 145
- Device mobility group setup, page 146
- Device mobility info setup, page 146
- Physical location setup, page 146
- Certificate setup, page 147
- Phone security profile setup, page 147
- SIP trunk security profile setup, page 147
- CUMA server security profile setup, page 147
- License Usage Report setup, page 148
- Geolocation setup, page 148
- Geolocation filter setup, page 148

BLF presence group setup

In Cisco Unified Communications Manager Administration, use the System > BLF Presence Group menu path to configure BLF presence groups.

When you configure BLF 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.

Cisco Unified Communications Manager controls which destinations a watcher can monitor with BLF presence groups. A BLF presence group contains watchers and the destinations that can be monitored by the watchers in the group. To allow watchers in one group to monitor directory numbers in other groups, you specify permission settings to allow or block (disallow) the BLF presence request. Presence authorization works with the BLF presence groups that are configured to ensure that a watcher has permission to monitor the status of a destination.
After you configure the BLF presence groups, you apply a BLF presence group to the following items in Cisco Unified Communications Manager Administration:

- Directory number—Presence entity for which you want status
- SIP trunk—Watcher
- Phone that is running SIP—Watcher
- Phone that is running SCCP—Watcher
- Application user—Watcher
- End user—Watcher

For information about configuring BLF presence groups, see the *Cisco Unified Communications Manager Features and Services Guide*.

**Device mobility group setup**

In Cisco Unified Communications Manager Administration, use the **System > Device Mobility > Device Mobility Group** menu path to configure device mobility groups.

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.

See topics related to device mobility group configuration in the *Cisco Unified Communications Manager Features and Services Guide* for more information on the Device Mobility feature.

**Device mobility info setup**

In Cisco Unified Communications Manager Administration, use the **System > Device Mobility > Device Mobility Info** menu path to configure device mobility info.

The Device Mobility Info 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 device mobility subnets that are specified in the Device Mobility Info window and associated with one of the device pools.

The matching subnet becomes the device home subnet for the purpose of device mobility.

See the *Cisco Unified Communications Manager Features and Services Guide* for more information on the Device Mobility feature.

**Physical location setup**

In Cisco Unified Communications Manager Administration, use the **System > Physical Location** menu path to configure physical locations.
Physical locations support the Device Mobility feature. Physical locations provide a means of distinguishing the parameters that relate to a specific geographical location from other parameters. For example, a media resources 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, you want to have the media resources server at the roaming location serve the device. By defining the physical location according to availability of media services, 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 may define physical locations based upon a city, enterprise campus, or building.

See topics related to physical location configuration in the Cisco Unified Communications Manager Features and Services Guide for more information on the device mobility feature.

**Certificate setup**

In Cisco Unified Communications Manager Administration, use the System > Security > Certificate menu path to configure certificates.

**Phone security profile setup**

In Cisco Unified Communications Manager Administration, use the System > Security > Phone Security Profile menu path to configure phone security profiles.

The Phone Security Profile window includes security-related settings such as device security mode, CAPF settings, digest authentication settings (only for phones that are running SIP), and encrypted configuration file settings. You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration.

For information on configuring and applying a phone security profile, see the Cisco Unified Communications Manager Security Guide.

**SIP trunk security profile setup**

In Cisco Unified Communications Manager Administration, use the System > Security > SIP Trunk Security Profile menu path to configure SIP trunk security profiles.

The SIP Trunk Security Profile window includes security-related settings such as transport type, device security mode, digest authentication settings, and authorization settings for incoming SIP messages. You must apply a security profile to all SIP trunks that are configured in Cisco Unified Communications Manager Administration.

For information on configuring and applying a SIP trunk security profile, see the Cisco Unified Communications Manager Security Guide.

**CUMA server security profile setup**

In Cisco Unified Communications Manager Administration, use the System > Security > CUMA Server Security Profile menu path to configure CUMA server security profiles.

The CUMA Server Security Profile window includes security-related settings such as device security mode, incoming transport type, and X.509 subject name. This security profile automatically gets applied to all Cisco
Unified Mobile Communicator clients that you configure in the device configuration window of Cisco Unified Communications Manager Administration.

For information on configuring a Cisco Unity Mobility Advantage (CUMA) server security profile, see the *Cisco Unified Communications Manager Security Guide*. For information on setting up a security profile for a CUMA server, see your Cisco Unified Mobility Advantage documentation. Make sure that the CUMA Security Profile you configure on Cisco Unified Communications Manager matches the security profile on the CUMA servers.

**License Usage Report setup**

In Cisco Unified Communications Manager Administration, use the **System > Licensing > License Usage Report** menu path to configure the license usage report.

**Geolocation setup**

In Cisco Unified Communications Manager Administration, use the **System > Geolocation Configuration** menu path to configure geographic locations for use with geographic location filters and logical partition policies to provision logical partitioning and other features.

**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.

For an explanation of geolocations, location conveyance, and configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For more information on how the logical partitioning feature uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.

**Geolocation filter setup**

In Cisco Unified Communications Manager Administration, use the **System > Geolocation Filter** menu path geographic location filters for use with geographic locations and logical partition policies to provision logical partitioning.

For an explanation of geolocations filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For more information on how the logical partitioning feature uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.
PART III

Call routing setup

- Automated alternate routing group setup, page 151
- Application dial rule setup, page 155
- Directory lookup dial rule setup, page 159
- SIP dial rule setup, page 161
- Route filter setup, page 169
- Route group setup, page 177
- Route list setup, page 183
- Route pattern setup, page 189
- Line group setup, page 201
- Hunt list setup, page 209
- Hunt pilot setup, page 215
- SIP route pattern setup, page 227
- Time period setup, page 233
- Time schedule setup, page 237
- Partition setup, page 241
- Calling search space setup, page 247
- Translation pattern setup, page 251
• Directory number setup, page 263
• Meet-Me number and pattern setup, page 297
• Dial plan installer, page 299
• Route plan report, page 305
• Calling party transformation pattern setup, page 311
• Called party transformation pattern setup, page 315
• Intercluster directory URI, page 319
• Other call routing menu options, page 325
Automated alternate routing group setup

This chapter provides information to find, add, update, or delete AAR groups.

For additional information, see topics related to Automated Alternate Routing in the Cisco Unified Communications Manager System Guide.

- About AAR group setup, page 151
- AAR group deletion, page 152
- AAR group settings, page 152

About AAR group setup

In Cisco Unified Communications Manager Administration, use the Call Routing > AAR Group menu path to configure AAR groups.

Automated alternate routing (AAR) provides a mechanism to reroute calls through the PSTN or other network by using an alternate number when Cisco Unified Communications Manager blocks a call due to insufficient location bandwidth. With automated alternate routing, the caller does not need to hang up and redial the called party. The AAR group represents the dialing area where the line/directory number (DN), the Cisco voice mail port, and the gateway are located.

For each AAR group, you enter the prefix digits that are used for automated alternate routing within the AAR group, as well as the prefix digits used for automated alternate routing between a given AAR group and other AAR groups. Devices, such as gateways, phones (by means of directory numbers), and trunks, associate with AAR groups. If automated alternate routing of calls takes place, you may also associate devices with an AAR calling search space.

Note

For AAR to function, you must configure AAR groups and also ensure that the Automated Alternate Routing Enable clusterwide service parameter is set to True. (The default value for this service parameter specifies False.)

See topics related to understanding route plans in the Cisco Unified Communications Manager System Guide for more information about automated alternate routing groups.
AAR group deletion

You cannot delete an AAR group that one or more devices references. To find out which devices are using the AAR group, choose the Dependency Records link from the Related Links drop-down list box that is on the AAR Group Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. You must remove the AAR group from all devices to which it belongs before deleting the AAR group.

Related Topics

Access dependency records, on page 874

AAR group settings

The following table describes the AAR group settings.

Table 24: AAR group settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Alternate Routing Group Information</td>
<td>Enter the name that you want to assign to the new AAR group. The name can contain up to 20 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). <strong>Timesaver</strong> Use concise and descriptive names for your AAR groups. The CompanyNameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify an AAR group. For example, CiscoDallasAA1 identifies a Cisco Access Analog AAR group for the Cisco office in Dallas.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name</td>
<td>Prefix Digits Within</td>
</tr>
<tr>
<td>Prefix Digits Between This Group and Other AAR Groups</td>
<td>Prefix Digits</td>
<td>Enter the prefix digits to use for automated alternate routing when routing a call from this group to a device that belongs to another AAR group. Valid entries include numeric characters (0-9), alpha characters (A-D), asterisk (*), and pound (#). Note Prefix digits that are entered in this field for the originating AAR group also get added in the Prefix Digits (To this group) field of the AAR destination group.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
Dial Prefix (To this group) | Enter the prefix digits to use for automated alternate routing when you are routing a call to this group from a device that belongs to another AAR group. Valid entries include numeric characters (0-9), alpha characters (A-D), asterisk (*), and pound (#). **Note** Prefix digits entered in this field for the destination AAR group also get added in the Prefix Digits (From this group) field of the AAR originating group.

**Related Topics**

Automated alternate routing group setup, on page 151
AAR group settings
Application dial rule setup

This chapter provides information to configure dial rules.
For additional information about dial rules, see Cisco Unified Communications Manager System Guide.

- About application dial rule setup, page 155
- Reprioritize dial rule, page 157

About application dial rule setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Dial Rules > Application Dial Rules menu path to configure application dial rules.

The administrator uses dial rules configuration to add and sort the priority of dialing rules. Dial rules for applications such as Cisco Unified Communications Manager Assistant automatically strip numbers from or add numbers to telephone numbers that a user dials. For example, the dial rules automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

For example, in Cisco Unified Communications Manager Assistant, the assistant can perform a directory search from the assistant console. The assistant can drag and drop the directory entry to the My Calls panel on the assistant console, which invokes a call to the number that is listed in the entry. The dial rules apply to the number that is listed in the entry before the call gets made.

Application dial rules configuration tips

When you perform the procedure to add a new dial rule or update an existing dial rule, see the Cisco Unified Communications Manager System Guide for dial rule design and error checking.

Note

If more than one dial rule exists, you can change the priority of the dial rules.

Related Topics

- Reprioritize dial rule, on page 157
Application dial rule settings

The following table describes the available settings in the Application Dial Rule Configuration window.

Table 25: Application dial rule settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name in the Name field. The name must be at least one character in length and can include up to 50 alphanumeric characters, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;). Ensure each application dial rule name is unique.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the application dial rule in the Description field. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Number Begins With</td>
<td>Enter the initial digits of the directory numbers to which you want to apply this application dial rule. Valid characters include numeric digits (0-9), plus sign (+), asterisk (*), and number sign (#). Be aware that you cannot enter more than 50 characters in this field. For information on special characters that can be used in this field, refer to the Wildcards and special characters in route patterns and hunt pilots section of the Understanding Route Plans chapter of the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>
| Number of Digits       | Enter the length of the dialed numbers to which you want to apply this application dial rule. This field  
  - Supports numeric characters (0-9) only.  
  - Must contain a value that is equal to or greater than 0 and less than 100.  |
| Total Digits to be Removed | Enter the number of digits that you want Cisco Unified Communications Manager to remove from the beginning of dialed numbers that apply to this dial rule. This field  
  - Supports numeric characters (0-9) only.  
  - Must contain a value that is equal to or greater than 0 and less than 100.  
  - Cannot contain a value that is more than the value in the Number of Digits field. |
Enter the pattern to prepend to dialed numbers that apply to this application dial rule. Valid values include numeric digits (0-9), plus (+), asterisk (*), and pound (#). Be aware that you cannot enter more than 50 characters in this field.

Choose the dial rule priority as top, bottom, or middle.

**Related Topics**

*Application dial rule setup, on page 155*

**Reprioritize dial rule**

Perform the following procedure to reprioritize a dial rule.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 1** | From Cisco Unified Communications Manager Administration, choose **Call Routing > Dial Rules > Application Dial Rules**.  
*Note* You can also change the priority by starting from the Application Dial Rules Configuration window. |
| **Step 2** | In the Find and List Application Dial Rules window, choose a dial rule and click the dial rule name. The Application Dial Rule Configuration window displays. |
| **Step 3** | Use the up and down arrows to move the dial rule up or down the list. |
| **Step 4** | When you complete prioritizing the order, click Save. |

**Related Topics**

*Application dial rule setup, on page 155*
Reprioritize dial rule
CHAPTER 29

Directory lookup dial rule setup

This chapter provides information about directory lookup dial rules configuration.

For additional information, see topics related to dial rules in the *Cisco Unified Communications Manager System Guide*.

- About directory lookup dial rule setup, page 159
  - Directory lookup dial rule settings, page 159

About directory lookup dial rule setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Dial Rules > Directory Lookup Dial Rules** menu path to configure directory lookup dial rules.

Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory. Each rule specifies which numbers to transform based on the beginning digits and length of the number. For example, you can create a directory lookup rule that automatically removes the area code and 2 prefix digits from a 10-digit telephone, which would transform 4085551212 into 51212. If Cisco Unified Communications Manager Attendant Console can match the number with a user in the speed-dial entries of the attendant or in the directory, the attendant console displays the name in the Call Detail window.

Directory lookup dial rule settings

The following table describes the available settings in the Phone Configuration window.

*Table 26: Directory lookup dial rule settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the directory lookup dial rule. The name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).</td>
</tr>
</tbody>
</table>
### Directory lookup dial rule settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a description of the directory lookup dial rule in the Description field or leave blank. 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>
<tr>
<td>Number Begins With</td>
<td>Enter the initial digits of the directory numbers to which you want to apply this directory lookup dial rule. For example, if you enter 972, this dial rule applies to directory numbers that include 9725551212. Valid values include numeric digits (0 through 9), plus (+), asterisk (*), and pound (#).</td>
</tr>
<tr>
<td>Number of Digits</td>
<td>Enter the length of the directory numbers to which you want to apply this directory lookup dial rule. For example, if you enter 7, this dial rule applies to directory numbers including 8675309.</td>
</tr>
<tr>
<td>Total Digits to be Removed</td>
<td>Enter the number of digits that you want Cisco Unified Communications Manager to remove from directory numbers that apply to this dial rule. For example, if you enter 3, Cisco Unified Communications Manager removes 408 from directory numbers that include 4085556666. Valid values for this field range from 1 to 100. The total digits to be removed cannot be more than the number of digits of the directory numbers that apply to this directory lookup dial rule.</td>
</tr>
</tbody>
</table>
| Prefix With Pattern  | Enter the pattern to prepend to directory numbers that apply to this directory lookup dial rule. Valid values include digits (0 through 9), plus (+), asterisk (*), and pound (#).  
**Note** If a prefix pattern is defined, the digits to be removed can equal 0. If the prefix pattern is not defined, the digits to be removed must be greater than 0. |

**Related Topics**

Directory lookup dial rule setup, on page 159
CHAPTER 30

SIP dial rule setup

This chapter provides information about SIP dial rules configuration.

For additional information, see topics related to dial rules in the Cisco Unified Communications Manager System Guide.

- About SIP dial rule setup, page 161
- SIP dial rules settings, page 162
- Set up SIP dial rule, page 164
- Reset SIP dial rule, page 167
- Synchronize SIP dial rule settings with SIP phones, page 168

About SIP dial rule setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Dial Rules > SIP Dial Rules menu path to configure SIP dial rules.

The administrator uses SIP dial rules configuration to configure dial plans for phones that are running SIP and associate them with the following phones that are running SIP:

- Cisco Unified IP Phone 7911, 7941, 7961, 7970, 7971, 9951 and 9971. These phones use the 7940_7960_OTHER dial rules patterns. Key Press Markup Language (KPML) allows the digits to be sent to Cisco Unified Communications Manager digit by digit; SIP Dial Rules allow a pattern of digits to be collected locally on the phone prior to sending to Cisco Unified Communications Manager. If SIP dial rules are not configured, KPML gets used. To increase the performance of Cisco Unified Communications Manager (increasing the number of calls that get processed), Cisco recommends that administrators configure SIP dial rules.

- Cisco Unified IP Phone 7940 and 7960. These phones use the 7940_7960_OTHER dial rules patterns and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must press the Dial softkey or wait a specified time before digits are sent to Cisco Unified Communications Manager for processing. This extra step for the user delays the actual call from being processed.

- Cisco Unified IP Phone 7905 and 7912. These phones use the 7905_7912 dial rules patterns and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must
press the Dial softkey or wait a specified time before digits are sent to Cisco Unified Communications Manager for processing. This extra step for the user delays the actual call from being processed.

If the administrator does not configure a dial plan for a phone that is running SIP, the user must press the Dial softkey unless the phone supports KPML. If the administrator configures SIP dial plans, those dial plans must get associated with a phone that is running SIP, so the dial plans get sent to the device.

Tip
When you add or update a SIP dial rule in Cisco Unified Communications Manager Administration, be aware that the Cisco TFTP service rebuilds all phone configuration files, which may cause CPU to spike on the server where the Cisco TFTP service runs, especially if you have a large system with many phones. To ensure that CPU does not spike, add or update the SIP dial rule during a maintenance window or temporarily stop the Cisco TFTP service in Cisco Unified Serviceability before you make the configuration change. If you stop the Cisco TFTP service, remember to restart the service in Cisco Unified Serviceability after you add or update the SIP dial rule.

SIP dial rules configuration tips
When you add or update a SIP dial rule in Cisco Unified Communications Manager Administration, be aware that the Cisco TFTP service rebuilds all phone configuration files, which may cause CPU to spike on the server where the Cisco TFTP service runs, especially if you have a large system with many phones. To ensure that CPU does not spike, add or update the SIP dial rule during a maintenance window or temporarily stop the Cisco TFTP service in Cisco Unified Serviceability before you make the configuration change. If you stop the Cisco TFTP service, remember to restart the service in Cisco Unified Serviceability after you add or update the SIP dial rule. See topics related to configuring a SIP dial rule for steps that supplement the standard procedure for configuring or updating a record in Cisco Unified Communications Manager Administration.

Related Topics
Set up SIP dial rule, on page 164

SIP dial rules settings
The following table describes the available settings in the SIP Dial Rules Configuration window.

Table 27: SIP dial rule settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial Pattern</td>
<td>Choose the dial pattern that is applicable to the type of phone that is running SIP that you have; for example, dial pattern 7905_7912 applies for Cisco Unified IP Phones 7905 and 7912, and dial pattern 7940_7960_OTHER applies for Cisco Unified IP Phones 7911, 7940, 7941, 7960, 7961, 7970, and 7971.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Cisco Unified IP Phones 7905, 7912, 7940, and 7960 do not support KPML.</td>
</tr>
<tr>
<td>SIP Dial Rule Information</td>
<td></td>
</tr>
</tbody>
</table>
### SIP dial rules settings

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the SIP dial rule; for example, Long Distance. Enter up to 50 alphanumeric characters including spaces and special characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a brief description of the dial rule.</td>
</tr>
<tr>
<td><strong>Pattern Information</strong></td>
<td></td>
</tr>
<tr>
<td>Pattern Description</td>
<td>Enter a name for the pattern description; for example, Emergency.</td>
</tr>
<tr>
<td>Delete Pattern</td>
<td>Check this check box to delete the dial pattern; then, click the Delete Selected button.</td>
</tr>
<tr>
<td><strong>Dial Parameter</strong></td>
<td>From this drop-down list box, choose the type of parameter for this pattern from the following choices:</td>
</tr>
<tr>
<td></td>
<td>• Pattern—Use this parameter for 7905_7912 and 7940_7960_OTHER dial rules. See the Pattern formats, on page 165 for specific pattern formats.</td>
</tr>
<tr>
<td></td>
<td>• Button—This parameter specifies the line button to which the dial pattern applies. If the user is initiating a call on line button 1, only the dial pattern that is specified for Button 1 applies. If this optional parameter is not configured, the dial pattern applies to all lines. It only applies to the Cisco Unified IP Phones 7940, 7941, 7960, 7961, 7970, and 7971. The administrator must enter a button number as the value. The button number corresponds to the order of the buttons on the side of the screen that is on the phone, from top to bottom, with 1 being on top. The Cisco Unified IP Phones 7940 and 7941 have two line buttons, the 7960 and 7961 have six line buttons, and the 7970 and 7971 have eight line buttons.</td>
</tr>
<tr>
<td></td>
<td>• Timeout—This parameter specifies the time, in seconds, before the system times out and dials the number as entered by the user. To have the number dial immediately, specify 0. Use this parameter only for 7940_7960_OTHER dial rules.</td>
</tr>
<tr>
<td></td>
<td>• User—This parameter represents the tag that automatically gets added to the dialed number. Valid values include IP and Phone for this tag that is not case sensitive. Use this parameter only for 7940_7960_OTHER dial rules.</td>
</tr>
<tr>
<td>Value</td>
<td>For the dial parameters that this table describes, enter the value for that field here. For example, enter 1 for Button 1 of PLAR, or 8,..... for a 7940_7960_OTHER pattern.</td>
</tr>
<tr>
<td>Delete Parameter</td>
<td>Check this check box to delete the dial pattern; then, click the Delete Selected button.</td>
</tr>
<tr>
<td>Edit Parameter</td>
<td>Click this button to update an existing parameter.</td>
</tr>
</tbody>
</table>
Field | Description
---|---
Add New Parameter | Click this button to add a new parameter to the pattern.
Delete Selected | Click this button to delete a parameter or a pattern.
Pattern Addition

Pattern Description | Enter a name for a new pattern; for example, Longdistance; then, click the Add Pattern or Add PLAR button.
Add Pattern | Click this button to add the new pattern to the Pattern Information pane.
Add PLAR | Click this button to add the new PLAR pattern to the Pattern Information pane.

Related Topics

SIP dial rule setup, on page 161

Set up SIP dial rule

Use the standard procedure for configuring or updating a new record when you are configuring or updating a SIP dial rule. The following steps also apply when you configure or update a SIP dial rule.

Procedure

**Step 1** From the Dial Pattern drop-down list box, choose either 7905_7912 or 7940_7960_OTHER as the SIP dial rule type.

**Step 2** Click the Next button. The SIP Dial Rule Configuration redisplay with updated information.

**Step 3** Enter a name and description of the Dial Rule that you are creating by using the information as described in Table 27: SIP dial rule settings, on page 162. Click Save. The SIP Dial Rule Configuration redisplay with updated information.

**Step 4** Enter a name for the pattern description by using the information as described in Table 27: SIP dial rule settings, on page 162.

**Step 5** Depending on the type of dial pattern that you want to create, click Add Pattern or Add PLAR (Private Line Automatic Ringdown [PLAR]).

**Note** The Add PLAR button only displays for 7940_7960_OTHER dial rules.

The SIP Dial Rule Configuration redisplay with updated information and an area to configure the dial pattern parameters.
Related Topics

SIP dial rule setup, on page 161
Pattern formats, on page 165
SIP dial rules examples, on page 166

Pattern formats

Formats are provided for the 7905_7912 and 7940_7960_OTHER patterns.

Value for 7905_7912 pattern

- Period (.) matches any digit.
- Hyphen (-) means more digits can be entered. If this character is needed, it must appear at the end of an individual rule. For example, 1408t5- is legal, but 1408t5-3... is illegal.
- Pound sign (#) acts as the terminating key, and termination can be applied only after matching hits >#. So >* means that the terminating character specifies the asterisk (*); that is, the terminating key must follow the greater-than sign (>).
- Characters "tn" set the timeout to n seconds.

Note

n equals 0-9, and a-z, which ranges from 0 to 26.

- Characters "rn" repeat the last pattern n times.

Note

The characters "->#" and "tn" specify modifiers, not patterns. n equals 0-9 and a-z, which ranges from 0 to 26. Use the repeat modifier to specify more rules in less space.

- Modifier "S" causes rule-matching to cease (that is, if a rule matches and the modifier "S" is seen, all other rules after that matching rule do not get used for matching).

Value for 7940_7960_OTHER pattern

- Period (.) matches any character.
- Pound sign (#) acts as the terminating key, and termination can be applied only after matching hits >#. So >* means that the terminating character specifies the asterisk (*); that is, the terminating key must follow the greater-than sign (>).

Note

You must configure the pound sign in the pattern field for it to be valid for 7940_7960_OTHER.
• Asterisk (*) matches one or more characters. The * gets processed as a wildcard character. You can override this by preceding the * with a backward slash (\) escape sequence, which results in the sequence \\*. The phone automatically strips the \, so it does not appear in the outgoing dial string. When * is received as a dial digit, it gets matched by the wildcard characters * and period (.).

• Comma (,) causes the phone to generate a secondary dial tone.

Example: 7.... will match any 4-digit DN that starts with 7. 8,..... will match 8, play secondary dial tone (default value), then match any 5-digit DN.

SIP dial rules examples

The following table provides some example SIP dial rules for the 7905_7912 dial rules.

Table 28: SIP dial rule examples for 7905_7912 dial rules

<table>
<thead>
<tr>
<th>Pattern String</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>.t7&gt;#......t4-</td>
<td>You must enter at least one digit. After that, the send occurs after 7 seconds. The terminating # character can also be applied after the first digit is entered. After 7 digits are entered, the timeout changes to 4 seconds. The _ character means that more digits can be entered, as long as timeout or # does not terminate the string.</td>
</tr>
<tr>
<td>911 and 9911</td>
<td>Send immediately. Configure a SIP dial rule for each of these strings, with the timeout dial parameter set to 0, to ensure that no delay occurs in sending the call. The user does not have to press the Dial softkey to initiate the call, even if the phone does not support Key Press Markup Language (KPML).</td>
</tr>
<tr>
<td>1t7&gt;#........t1-</td>
<td>You must enter at least one digit. After that, the send occurs after 7 seconds. The terminating character # can also be applied after the first digit is entered. After 10 digits are entered, the timeout changes to 1 second. The _ character means that more digits can be entered, as long as timeout or # does not terminate the string.</td>
</tr>
<tr>
<td>0t4&gt;#.t7-&quot;</td>
<td>After a 0, if no other digit is entered, the send occurs after 4 seconds. If another digit is entered, send occurs after 7 seconds. Again, # acts as the terminating digit.</td>
</tr>
</tbody>
</table>

The following table provides some example SIP dial rules for the 7940_7960_OTHER dial rules.

Table 29: SIP dial rule examples for 7940_7960_OTHER dial rules

<table>
<thead>
<tr>
<th>Pattern String</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>123#45#6</td>
<td>The 123#45#6 string gets matched if the user dials 123#45#6. Pressing the pound sign (#) does not cause the phone to dial immediately because # is explicitly specified. For Cisco SIP IP Phones 7940 and 7960, dialing 1# or 123#4# causes the phone to dial immediately.</td>
</tr>
</tbody>
</table>
Effect Pattern String | Effect
--- | ---
911 and 9911 | Send immediately. Configure a SIP dial rule for each of these strings, with the timeout dial parameter set to 0, to ensure that no delay occurs in sending the call. The user does not have to press the Dial softkey to initiate the call, even if the phone does not support Key Press Markup Language (KPML).
12\*345 | This example uses the backward slash (\) and asterisk (*) to indicate that the asterisk (*) is a dialed digit. If you omit the backslash (\), the asterisk(*) gets treated as a wildcard pattern match. If you use the backslash (\) with a character other than the asterisk (*), the \ gets ignored, and the \ character gets matched. If you need to explicitly specify the \ character in a dial plan, use \\. The \ does not get sent out as part of the dialed digit string because the phone removes it before it sends the dial string.

**Reset SIP dial rule**

Perform the following procedure to reset or restart the phone that is running SIP when the SIP dial rule gets updated, so the phone gets updated with the new SIP dial rule.

**Procedure**

**Step 1**
From Cisco Unified Communications Manager Administration, choose Call Routing > Dial Rules > SIP Dial Rules.

**Step 2**
Locate the SIP dial rule that you want to reset.

**Step 3**
Click the SIP dial rule that you want to reset.
The SIP Dial Rule Configuration window displays.

**Step 4**
Click Reset.
The Device Reset dialog displays.

**Step 5**
Click one of the following choices:

a) Restart—Restarts the chosen devices without shutting them down (reregisters the phones with Cisco Unified Communications Manager).
b) Reset—Shuts down, then restarts, the device.
c) Close—Closes the Device Reset dialog without performing any action.

**Related Topics**

SIP dial rule setup, on page 161
About SIP dial rule setup, on page 161
Synchronize SIP dial rule settings with SIP phones

To synchronize a SIP phone with a SIP Dial Rule that has undergone configuration changes, perform the following procedure, which applies any outstanding configuration settings in the least intrusive manner possible. (For example, a reset/restart may not be required on some affected SIP phones.)

**Procedure**

**Step 1** Choose Device > Dial Rules > SIP Dial Rule.
The Find and List SIP Dial Rules window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find.
The window displays a list of SIP Dial Rules that match the search criteria.

**Step 4** Click the SIP Dial Rule to which you want to synchronize applicable SIP phones. The SIP Dial Rule 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.

**Related Topics**

SIP dial rule setup, on page 161
Route filter setup

This chapter provides information to add, update, copy, or delete a route filter. For additional information about route plans, see the Cisco Unified Communications Manager System Guide.

- About route filter setup, page 169
- Route filter deletion, page 170
- Route filter settings, page 170
- Add and edit route filter clauses, page 171
- Remove route filter clauses, page 172
- Synchronize route filter settings with devices, page 172
- Route filter tag descriptions, page 173

About route filter setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Route Filter menu path to configure route filters.

Route filters, along with route patterns/hunt pilots, use dialed-digit strings to determine how a call is handled. Route filters only apply when you configure a pattern that contains the @ wildcard. When the route pattern/hunt pilot contains the @ wildcard, Cisco Unified Communications Manager routes calls according to the numbering plan that is specified in the Numbering Plan drop-down list box. The route filter window that Cisco Unified Communications Manager displays varies according to the numbering plan that you select.

Route filters allow you to determine which route patterns/hunt pilots your users can dial; for example, whether your users can manually choose a long-distance carrier (by dialing 101 plus a carrier access code).

See topics related to understanding route plans in the Cisco Unified Communications Manager System Guide for more information.

Tip

Always add and define the route filter first and then add the route filter to the route pattern/hunt pilot.
**Route filter configuration tips**

Synchronize a route filter with affected devices after you configure or update a route filter.

After you configure or update a route filter, see topics related to adding, editing, and removing route filter clauses.

**Related Topics**

- Add and edit route filter clauses, on page 171
- Remove route filter clauses, on page 172
- Synchronize route filter settings with devices, on page 172

**Route filter deletion**

You cannot delete a route filter that route patterns/hunt pilots, translation patterns, or other items use. To find out which route patterns/hunt pilots, translation patterns, or other items are using the route filter, in the Route Filter Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a route filter that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a route filter that is currently in use, you must perform either or both of the following tasks:

- Assign a different route filter to any route patterns/hunt pilots, translation patterns, or other items that are using the route filter that you want to delete.
- Delete the route patterns/hunt pilots, translation patterns, or other items that are using the route filter that you want to delete.

**Related Topics**

- About route pattern setup, on page 189
- About translation pattern setup, on page 251
- Translation pattern deletions, on page 252
- Access dependency records, on page 874

**Route filter settings**

The following table describes the route filter settings.

*Table 30: Route filter settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numbering Plan</td>
<td>From the drop-down list, choose a dial plan; for example, North American Numbering Plan. Click Next.</td>
</tr>
</tbody>
</table>

| Route Filter Information |
Add and edit route filter clauses

Adding route filter clauses allows you to expand upon an existing route filter by incorporating additional operators and entries for existing tags by using a logical OR. You can add route filter clauses either when initially adding a new route filter or when updating an existing route filter.

Editing route filter clauses allows you to modify an existing route filter clause.

This procedure describes adding and editing route filter clauses that comprise an existing route filter.

Procedure

1. From Cisco Unified Communications Manager Administration, choose Call Routing > Route Filter.
2. Locate the route filter to which you want to add or edit route filter clauses.
3. If you want to add a new route filter clause, click Add Clause to display a new Route Filter Clause Configuration data entry window. All the operator fields for this new clause display NOT-SELECTED.
4. Choose the route filter tags and operators and enter data, where appropriate, to create an additional clause for this route filter.
Remove route filter clauses

You can remove route filter clauses either when setting up a new route filter or when updating an existing route filter. This procedure describes removing a route filter clause from an existing route filter.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose Call Routing > Route Filter.

Step 2 Locate the route filter from which you want to remove route filter clauses.

Step 3 Scroll down to the top of the clause that you want to remove and click Remove Clause.

Caution Each Remove Clause button applies to the clause immediately below the button. Check carefully to ensure that you are removing the correct clause before initiating this action. If you accidentally remove a clause, you cannot retrieve it, and you must rebuild it.

Step 4 To remove the clause, click OK or to cancel the action, click Cancel. If you click OK, Cisco Unified Communications Manager removes the clause from the route filter.

Related Topics

Route filter setup, on page 169
Procedure

**Step 1** Choose **Call Routing** > **Route Filter**.
The Find and List Route Filters window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find.
The window displays a list of route filters that match the search criteria.

**Step 4** Click the route filter to which you want to synchronize applicable devices. The Route Filter 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** Any necessary resetting of devices that are associated with the route filter causes calls on affected gateways to drop.

**Step 8** Click OK.

Related Topics

*Route filter setup, on page 169*

**Route filter tag descriptions**

The tag serves as the core component of a route filter. A tag applies a name to a subset of the dialed-digit string. For example, the NANN number 972-555-1234 comprises LOCAL-AREA-CODE (972), OFFICE-CODE (555), and SUBSCRIBER (1234) route filter tags.

Route filter tags require operators and can require additional values to decide which calls are filtered.

The values for route filter tag fields can contain the wildcard characters X, *, #, [ ], ^, - , ^, and the numbers 0 through 9. (See topics related to special characters and settings for route filters in the *Cisco Unified Communications Manager System Guide* for definitions of wildcard characters.) The descriptions in The following table use the notations [2-9] and XXXX to represent actual digits. In this notation, [2-9] represents any single digit in the range 2 through 9, and X represents any single digit in the range 0 through 9. Therefore, the description The three-digit area code in the form [2-9]XX" means that you can enter the actual digits 200 through 999, or all wildcards, or any mixture of actual digits and wildcards that results in a pattern with that range.

Route filter tags vary depending on the numbering plan that you choose from the Numbering Plan drop-down list box on the Route Filter Configuration window. The following table describes the route filter tags for the North American Numbering Plan.
Table 31: Route filter tags

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AREA-CODE</td>
<td>This three-digit area code in the form [2-9]XX identifies the area code for long-distance calls.</td>
</tr>
<tr>
<td>COUNTRY CODE</td>
<td>These one-, two-, or three-digit codes specify the destination country for international calls.</td>
</tr>
<tr>
<td>END-OF-DIALING</td>
<td>This single character identifies the end of the dialed-digit string. The # character serves as the end-of-dialing signal for international numbers that are dialed within the NANP.</td>
</tr>
<tr>
<td>INTERNATIONAL-ACCESS</td>
<td>This two-digit access code specifies international dialing. Calls that originate in the U.S. use 01 for this code.</td>
</tr>
<tr>
<td>INTERNATIONAL-DIRECT-DIAL</td>
<td>This one-digit code identifies a direct-dialed international call. Calls that originate in the U.S. use 1 for this code.</td>
</tr>
<tr>
<td>INTERNATIONAL-OPERATOR</td>
<td>This one-digit code identifies an operator-assisted international call. This code specifies 0 for calls that originate in the U.S.</td>
</tr>
<tr>
<td>LOCAL-AREA-CODE</td>
<td>This three-digit local area code in the form [2-9]XX identifies the local area code for 10-digit local calls.</td>
</tr>
<tr>
<td>LOCAL-DIRECT-DIAL</td>
<td>This one-digit code identifies a direct-dialed local call. NANP calls use 1 for this code.</td>
</tr>
<tr>
<td>LOCAL-OPERATOR</td>
<td>This one-digit code identifies an operator-assisted local call. NANP calls use 0 for this code.</td>
</tr>
<tr>
<td>LONG-DISTANCE-DIRECT-DIAL</td>
<td>This one-digit code identifies a direct-dialed, long-distance call. NANP calls use 1 for this code.</td>
</tr>
<tr>
<td>LONG-DISTANCE-OPERATOR</td>
<td>These one- or two-digit codes identify an operator-assisted, long-distance call within the NANP. Operator-assisted calls use 0 for this code, and operator access uses 00.</td>
</tr>
<tr>
<td>NATIONAL-NUMBER</td>
<td>This tag specifies the nation-specific part of the digit string for an international call.</td>
</tr>
<tr>
<td>OFFICE-CODE</td>
<td>This tag designates the first three digits of a seven-digit directory number in the form [2-9]XX.</td>
</tr>
<tr>
<td>SATELLITE-SERVICE</td>
<td>This one-digit code provides access to satellite connections for international calls.</td>
</tr>
<tr>
<td>SERVICE</td>
<td>This three-digit code designates services such as 911 for emergency, 611 for repair, and 411 for information.</td>
</tr>
</tbody>
</table>
This tags specifies the last four digits of a seven-digit directory number in the form XXXX.

This four-digit value identifies a long-distance carrier. Do not include the leading 101 carrier access code prefix in the TRANSIT-NETWORK value. See TRANSIT-NETWORK-ESCAPE for more information.

This three-digit value precedes the long-distance carrier identifier. The value for this field specifies 101. Do not include the four-digit carrier identification code in the TRANSIT-NETWORK-ESCAPE value. See TRANSIT-NETWORK for more information.

Route filter tag operators determine whether a call is filtered based on the existence, and sometimes the contents, of the dialed-digit string that is associated with that tag. The operators EXISTS and DOES-NOT-EXIST simply check for the existence of that part of the dialed-digit string. The operator == matches the actual dialed digits with the specified value or pattern. The following table describes the operators that can be used with route filter tags.

### Table 32: Route filter operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOT-SELECTED</td>
<td>Specifies do not filter calls based on the dialed-digit string that is associated with this tag.</td>
</tr>
<tr>
<td></td>
<td>The presence or absence of the tag with which the operator is associated does not prevent Cisco Unified Communications Manager from routing the call.</td>
</tr>
<tr>
<td>EXISTING</td>
<td>Specifies filter calls when the dialed-digit string that is associated with this tag is found.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager routes or blocks the call only if the dialed-digit string contains a sequence of digits that are associated with the tag.</td>
</tr>
<tr>
<td>DOES-NOT-EXIST</td>
<td>Specifies filter calls when the dialed-digit string that is associated with this tag is not found.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager routes or blocks the call only if the dialed-digit string does not contain a sequence of digits that are associated with the tag.</td>
</tr>
<tr>
<td>==</td>
<td>Specifies filter calls when the dialed-digit string that is associated with this tag matches the specified value.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager routes or blocks the call only if the dialed-digit string contains a sequence of digits that are associated with the tag and within the numbering range that is specified in the attached field.</td>
</tr>
</tbody>
</table>
Caution
Do not enter route filter tag values for tags that are using the operators EXISTS, DOES-NOT-EXIST, or NOT-SELECTED.

Route filter examples

Example 1: A route filter that uses AREA-CODE and the operator DOES-NOT-EXIST selects all dialed-digit strings that do not include an area code.

Example 2: A route filter that uses AREA-CODE, the operator ==, and the entry 515 selects all dialed-digit strings that include the 515 area code.

Example 3: A route filter that uses AREA-CODE, the operator ==, and the entry 5[2-9]X selects all dialed-digit strings that include area codes in the range of 520 through 599.

Example 4: A route filter that uses TRANSIT-NETWORK, the operator ==, and the entry 0288 selects all dialed-digit strings with the carrier access code 1010288.

Related Topics
Route filter setup, on page 169
Route group setup

This chapter provides information to add or delete a route group or to add devices to or to remove devices from a route group.

For additional information about route plans, see the Cisco Unified Communications Manager System Guide. See the Cisco Unified Communications Manager Features and Services Guide for additional information about local route groups.

- About route group setup, page 177
- Route group deletion, page 178
- Route group settings, page 178
- Add devices to route group, page 180
- Remove devices from route group, page 181

About route group setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Route/Hunt Route Group menu path to configure route groups.

**Route/Hunt**

A route group allows you to designate the order in which gateways and trunks are selected. It allows you to prioritize a list of gateways and ports for outgoing trunk selection.

For example, if you use two long-distance carriers, you could add a route group, so long-distance calls to the less expensive carrier are given priority. Calls route to the more expensive carrier only if the first trunk is unavailable.

**Note**

For information about configuring the Local Route Group feature, see the Cisco Unified Communications Manager Features and Services Guide.

**Route group configuration tips**

After you configure a route group, see the following topics to add or remove devices from a route group:
• Add devices to route group, on page 180
• Remove devices from route group, on page 181

Route group deletion

You cannot delete a route group that a route/hunt list references. To find out which route lists are using the route group, in the Route Group Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a route group that is in use, Cisco Unified Communications Manager displays a message. Before deleting a route group that is currently in use, you must perform the following task:

• Remove the route group from all route lists to which it belongs before deleting the route group.

Tip
To delete route groups and route patterns, first delete the route pattern; second, delete the route list; and finally, delete the route group.

Related Topics
Remove route groups from route list, on page 187
Access dependency records, on page 874

Route group settings

The following table describes the route group settings.

Table 33: Route group settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Group Information</td>
<td></td>
</tr>
<tr>
<td>Route Group Name</td>
<td>Enter a name for this route group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan. Timesaver Use concise and descriptive names for your route groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route group. For example, CiscoDallasAA1 identifies a Cisco Access Analog route group for the Cisco office in Dallas.</td>
</tr>
</tbody>
</table>
Choose a distribution algorithm from the options in the drop-down list box:

- **Top Down**—If you choose this distribution algorithm, Cisco Unified Communications Manager distributes a call to idle or available members starting from the first idle or available member of a route group to the last idle or available member.

- **Circular**—If you choose this distribution algorithm, Cisco Unified Communications Manager distributes a call to idle or available members starting from the \((n+1)\)th member of a route group, where the \(n\)th member is the member to which Cisco Unified Communications Manager most recently extended a call. If the \(n\)th member is the last member of a route group, Cisco Unified Communications Manager distributes a call starting from the top of the route group.

The default value specifies Circular.

### Route Group Member Information

**Find Devices to Add to Route Group**

**Device Name contains**

Enter the character(s) that are found in the device name that you are seeking and click the Find button. Device names that match the character(s) that you entered display in the Available Devices box.

**Note** To find all available devices, leave the text box blank and click the Find button.

**Available Devices**

Choose a device in the Available Devices list box and add it to the Selected Devices list box by clicking Add to Route Group.

If the route group contains a gateway that uses the QSIG protocol, only gateways that use the QSIG protocol display in the list. If the route group contains a gateway that uses the non-QSIG protocol, gateways that use the controlled intercluster trunks, which are QSIG protocol, do not display in the list.

If you included the route group in a route list that contains QSIG gateways, the H.323 gateways do not display in the list.

**Port(s)**

If this device supports individually configurable ports, choose the port. (Devices that allow you to choose individual ports include Cisco Access Analog and Cisco MGCP Analog gateways and T1 CAS.) Otherwise, choose the default value (All or None Available, depending upon the device that is chosen). For a device that has no ports available (None Available), the device may already be added to the Route Group or cannot be added to the route group.

### Current Route Group Members
To change the priority of a device, choose a device name in the Selected Devices list box. Move the device up or down in the list by clicking the arrows on the right side of the list box.

To reverse the priority order of the devices in the Selected Devices list box, click Reverse Order of Selected Devices.

For more information about the order of devices in a route group, see topics related to route plan overview in the Cisco Unified Communications Manager System Guide.

Choose a device in the Selected Devices list box and add it to the Removed Devices list box by clicking the down arrow button between the two list boxes.

Note: You must leave at least one device in a route group.

This pane displays links to the devices that have been added to this route group. Click one of the device names to go to the configuration window for that particular device.

Note: When you are adding a new route group, this list does not display until you save the route group.

Related Topics

Route group setup, on page 177

Add devices to route group

You can add devices to a new route group or to an existing route group. You can add gateways to multiple route groups. After you add a gateway to any route group, the gateway does not display in the Route Pattern configuration window. The following procedure describes adding a device to an existing route group.

Before You Begin

You must define one or more gateway and trunk devices before performing this procedure. A device can reside in only one route group.
### Remove devices from route group

You can remove devices from a new route group or from an existing route group. The following procedure describes removing a device from an existing route group.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <em>Call Routing &gt; Route/Hunt &gt; Route Group.</em></td>
</tr>
<tr>
<td>Step 2</td>
<td>Locate the route group from which you want to remove a device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Selected Devices list box, choose a device to be removed and click the Down arrow below the Selected Devices list box to move the device to the Removed Devices list box. Repeat this step for each device that you want to remove from this route group. <strong>Note</strong> You must leave at least one device in a route group.</td>
</tr>
<tr>
<td>Step 4</td>
<td>To remove the devices, click Save.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Route group setup, on page 177
Remove devices from route group
Route list setup

This chapter provides information to add or delete route lists or to add, remove, or change the order of route groups in a route list.

For additional information about route plans, see the *Cisco Unified Communications Manager System Guide*.

For additional information about local route groups and how presence works with route lists, see the *Cisco Unified Communications Manager Features and Services Guide*.

- About route list setup, page 183
- Route list deletion, page 184
- Route list settings, page 184
- Add route groups to route list, page 185
- Remove route groups from route list, page 187
- Change route group order in route list, page 187
- Synchronize route list settings with route groups, page 188

**About route list setup**

In Cisco Unified Communications Manager Administration, use the Call Routing > Route/Hunt > Route List menu path to configure route lists.

A route list associates a set of route groups in a specified priority order. A route list then associates with one or more route patterns and determines the order in which those route groups are accessed. The order controls the progress of the search for available devices for outgoing calls.

A route list can contain only route groups. Each route list should have at least one route group. Each route group includes at least one device, such as a gateway, that is available. Based on device type, Cisco Unified Communications Manager can choose some, or all, ports as resources in each route group. Some devices, such as digital access, only allow you to choose all ports.

You can add a route group to any number of route lists.
**Route list configuration tips**

To begin configuration of a new route list, click the Add New button to display the Route List Configuration window where you configure the new route list.

After you configure a new route list, add at least one route group to the new route list.

After you configure a route list, continue configuration of the route list.

**Related Topics**

- Add route groups to route list, on page 185

---

**Route list deletion**

The Cisco Unified Communications Manager associates a route list with a route pattern. You cannot delete a route list if it associates with a route pattern. To find out which route patterns are using the route list, click the Dependency Records link from the Route List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

---

**Tip**

To delete route groups and route patterns, first delete the route pattern; second, delete the route list, and finally, delete the route group.

**Related Topics**

- Access dependency records, on page 874

---

**Route list settings**

The following table describes the route list settings.

**Table 34: Route list settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Route List Information</strong></td>
<td></td>
</tr>
<tr>
<td>Route List Name</td>
<td>Enter a name for this route list. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each route list name is unique to the route plan. <strong>Warning</strong> Use concise and descriptive names for your route lists. The CompanynameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a route list. For example, CiscoDallasMetro identifies a route list for toll-free, inter-local access transport area (LATA) calls from the Cisco office in Dallas.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this route list.</td>
</tr>
</tbody>
</table>
From this drop-down list box, choose a Cisco Unified Communications Manager group.

**Note** The route list registers with the first Cisco Unified Communications Manager in the group, which is its primary Cisco Unified CM.

If you choose a Cisco Unified CM group that has only one configured Cisco Unified CM, you receive the following warning:

**WARNING!** The selected Cisco Unified Communications Manager Group has only one Cisco Unified Communications Manager configured. For the control process to have redundancy protection, please select a Cisco Unified Communications Manager Group with more than one Cisco Unified Communications Manager.

**Enable this Route List**

By default, the system checks this check box for a new route list.

If you want to disable this route list, uncheck this check box. A popup window explains that calls in progress do not get affected, but this route list will not accept additional calls.

**Run On All Active Unified CM Nodes**

To enable the active route list to run on every node, check this check box.

**Save**

When you click this button to save a route list, a popup message reminds you that you must add at least one route group to this route list for it to accept calls.

**Add Route Group**

To add a route group to this route list, click this button and perform the procedure to add a route group to a route list.

**Note** For called party and calling party transformation information, you can click the name of a route group that belongs to this route list. The route group names display in the Route List Details list box at the bottom of the Route List Configuration window. This action displays the Route List Detail Configuration window for the route group that you choose.

**Related Topics**

- Route list setup, on page 183
- Add route groups to route list, on page 185

## Add route groups to route list

You can add route groups to a new route list or to an existing route list. Route groups can exist in one or more route lists. The following procedure describes adding a route group to an existing route list.
You cannot add route groups that contain MGCP gateways that use the QSIG protocol (a QSIG route group) and route groups that contain gateways that use the H.323 protocol (H.323 route group) to the same route list. For more information, see topics related to route groups and route lists in the *Cisco Unified Communications Manager System Guide*.

**Before You Begin**

Before performing this procedure, you must build one or more route groups and add a route list.

**Procedure**

**Step 1** Choose Call Routing > Route/Hunt > Route List.

**Step 2** Locate the route list to which you want to add route group.

**Step 3** To add a route group, click Add Route Group. The Route List Detail Configuration window displays.

**Step 4** From the Route Group drop-down list box, choose a route group to add to the route list.

**Note** If the route list contains a QSIG route group, H.323 route groups do not display in the drop-down list box. If the route group contains a H.323 route group, QSIG route groups do not display in the drop-down list box.

**Note** See topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide* for details.

**Step 5** If you need to manipulate the calling party number on calls that are routed through this route group, set up the calling party transformations in the appropriate fields.

**Note** For more information on calling party transformations, see the *Cisco Unified Communications Manager System Guide*.

**Step 6** If you need to manipulate the dialed digits on calls that are routed through this route group, set up the called party transformations in the appropriate fields.

**Note** For more information on called party transformations, see the *Cisco Unified Communications Manager System Guide*.

**Step 7** To add the route group, click Save. The route group details information appears in the Route List Details link.

**Step 8** To add more route groups to this list, click Add Route Group and repeat Step 3, on page 186 through Step 7, on page 186.

**Step 9** When you finish adding route groups to the route list, click Save.

**Note** See topics related to synchronizing a route list with the affected route groups before deciding whether to proceed to Step 10, on page 186 below.

**Step 10** Click Reset for changes to take effect. When the popup windows display, click Reset.

**Related Topics**

- Route list setup, on page 183
- Synchronize route list settings with route groups, on page 188
Remove route groups from route list

You can remove route groups from a new route list or from an existing route list. The following procedure describes removing a route group from an existing route list.

Procedure

Step 1 Choose Call Routing > Route/Hunt > Route List in the menu bar.
Step 2 Locate the route list from which you want to remove a route group.
Step 3 From the Selected Groups list, choose a route group name.
   Note To select multiple route groups from the list, press the Shift key and click the desired route groups.
Step 4 Click the Down Arrow below the Selected Groups list box to move the selected route group to the Removed Groups list.
Step 5 To remove the route group, click Save.
   When the window refreshes, click OK to remove the route group from the route list.
Step 6 Click Reset for the changes to take effect. Click Reset in response to the popup windows.

Related Topics

Route list setup, on page 183

Change route group order in route list

Cisco Unified Communications Manager accesses route groups in the order in which they appear in the route list. The following procedure allows you to change the access order of route groups.

Procedure

Step 1 Choose Call Routing > Route/Hunt > Route List.
Step 2 Locate the route list in which you want to change the order of a route group.
Step 3 From the Selected Groups list, choose a route group.
Step 4 To move the route group up or down in the list, choose a route group; then, click the up or down arrows on the right side of the list box.
Step 5 Click Save.
   Note For called party and calling party transformation information, click the route group icon or route group name in the Route List Details list at left. This action takes you to the Route List Detail Configuration window for the corresponding route group.
Step 6 Click Reset for the changes to take effect. Click Reset in response to the popup windows.
Related Topics

Route list setup, on page 183

Synchronize route list settings with route groups

To synchronize route groups with a route list that has undergone configuration changes, perform the following procedure, which applies any outstanding configuration settings in the least-intrusive manner possible. (For example, a reset/restart may not be required on some affected devices.)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Call Routing &gt; Route/Hunt &gt; Route List</strong>. The Find and List Route Lists window displays.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose the search criteria to use and click Find. The window displays a list of route lists that match the search criteria.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check the check boxes next to the route lists to which you want to synchronize applicable route groups. To choose all route lists in the window, check the check box in the matching records title bar.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Apply Config to Selected</strong>. The Apply Configuration Information dialog displays.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>

Related Topics

Route list setup, on page 183
Route pattern setup

This chapter provides information to find, add, update, copy, or delete a route pattern.

For additional information, see topics related to wildcards and special characters in route patterns and hunt pilots in the Cisco Unified Communications Manager System Guide, as well as topics related to route plans and route filter configuration.

For additional information about local route groups, see the Cisco Unified Communications Manager Features and Services Guide.

- About route pattern setup, page 189
- Route pattern settings, page 190

About route pattern setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Route/Hunt > Route Pattern menu path to configure route patterns.

A route pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a route list or a gateway. Route patterns provide flexibility in network design. They work in conjunction with route filters and route lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

See topics related to understanding route plans in the Cisco Unified Communications Manager System Guide for more detailed route pattern information.

Note

See topics related to local route groups in the Cisco Unified Communications Manager Features and Services Guide for a discussion of route patterns and their use and configuration when the Local Route Group feature is configured.

Route pattern configuration tips

Before you begin, ensure that the following items are configured in Cisco Unified Communications Manager:

- Gateway
• Route list
• Partition (unless you are using <None>)
• Route filter (unless you are using <None>)

**Timesaver** Assigning 8XXX to a gateway routes all directory numbers 8000 to 8999 out the gateway. Similarly, 82XX routes directory numbers 8200 to 8299. See topics related to special characters and settings in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.

---

**Note** If you change the gateway or route list, you must click Save prior to choosing the Edit link. Otherwise, you get linked to the previous gateway or route list.

**Note** The (Edit) link next to the Gateway or Route List field takes you to the Gateway Configuration or Route List Configuration window for reference, depending on whether the Gateway or Route List field contains a gateway or a route list. The Gateway Configuration window displays devices that are associated with the specified gateway. The Route List Configuration window displays the route groups that are associated with the specified route list.

---

**Route pattern settings**

The following table describes the available fields in the Route Pattern Configuration window.

*Table 35: Route pattern settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Definition</td>
<td></td>
</tr>
<tr>
<td>Route Pattern</td>
<td>Enter the route pattern, including numbers and wildcards (do not use spaces); for example, for 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 +.</td>
</tr>
</tbody>
</table>

**Note** Ensure that the directory route pattern, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. See topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.
If you want to use a partition to restrict access to the route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the route pattern, 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, then find and choose a partition name.

Note: To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Note: Make sure that the combination of route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.

Enter a description of the route pattern. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).

Choose a numbering plan.

If your route pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns.

The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.

You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name.

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>Route Partition</td>
<td>If you want to use a partition to restrict access to the route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the route pattern, choose &lt;None&gt; 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, then find and choose a partition name. Note: To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters. Note: Make sure that the combination of route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the route pattern. 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>
<tr>
<td>Numbering Plan</td>
<td>Choose a numbering plan.</td>
</tr>
<tr>
<td>Route Filter</td>
<td>If your route pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns. The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name. Note: To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MLPP Precedence</td>
<td>Choose an MLPP precedence setting for this route pattern from the drop-down list box:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Apply Call Blocking Percentage</td>
<td>Check this check box to enable the Destination Code Control (DCC) feature. By enabling DCC, all calls other than flash and higher precedence calls made to the destination are filtered and allowed or disallowed based on the Call Blocking Percentage quota set for the destination. Flash and higher precedence calls are allowed at all times. DCC is disabled by default.</td>
</tr>
<tr>
<td>Call Blocking Percentage (%)</td>
<td>Enter the percentage of calls to be blocked for this destination in numerals. This value specifies the percentage of lower precedence calls made to this destination that get blocked by the route pattern. This percentage limits the lower precedence calls only; the flash and higher precedence calls made to this destination are allowed at all times.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In Cisco Unified Communications Manager, you enable external call control by assigning an external call control profile to a route pattern. If the route pattern has an external call control profile assigned to it, when a call occurs that matches the route 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. For more information on external call control, see topics related to external call control in the *Cisco Unified Communications Manager Features and Services Guide*.

From the drop-down list box, choose the external call profile that you want to assign to the route pattern.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Call Control Profile</td>
<td>In Cisco Unified Communications Manager, you enable external call control by assigning an external call control profile to a route pattern. If the route pattern has an external call control profile assigned to it, when a call occurs that matches the route 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. For more information on external call control, see topics related to external call control in the <em>Cisco Unified Communications Manager Features and Services Guide</em>. From the drop-down list box, choose the external call profile that you want to assign to the route pattern.</td>
</tr>
<tr>
<td>Route Class</td>
<td>Choose a route class setting for this translation pattern from the drop-down list box:</td>
</tr>
<tr>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td></td>
<td>• Voice</td>
</tr>
<tr>
<td></td>
<td>• Data</td>
</tr>
<tr>
<td></td>
<td>• Satellite Avoidance</td>
</tr>
<tr>
<td></td>
<td>• Hotline voice</td>
</tr>
<tr>
<td></td>
<td>• Hotline data</td>
</tr>
<tr>
<td>Gateway/Route List</td>
<td>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 can 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. If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class. Choose the gateway or route list for which you are adding a route pattern.</td>
</tr>
<tr>
<td>Note</td>
<td>If the gateway is included in a Route Group, this drop-down list box does not display the gateway. When a gateway is chosen in the drop-down list box, Cisco Unified Communications Manager uses all the ports in the gateway to route/block this route pattern. This action does not apply for MGCP gateways.</td>
</tr>
</tbody>
</table>
### Route pattern settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Route Option   | The Route Option designation indicates whether you want this route 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. If you choose the Block this pattern radio button, you must choose the reason for which you want this route pattern to block calls. Choose a value from the drop-down list box:  
  - No Error  
  - Unallocated Number  
  - Call Rejected  
  - Number Changed  
  - Invalid Number Format  
  - Precedence Level Exceeded |
| Call Classification | Call Classification indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network. The default value specifies OffNet. When adding a route pattern, if you uncheck the Provide Outside Dial Tone check box, you set Call Classification as OnNet. |
| Allow Device Override | This check box remains unchecked by default. When the check box is checked, the system uses the Call Classification setting that is configured on the associated gateway or trunk to consider the outgoing call as OffNet or OnNet. |
| Provide Outside Dial Tone | Check this check box to provide outside dial tone. To route the call in the network, leave the check box unchecked. |
| Allow Overlap Sending | With overlap sending enabled, when Cisco Unified Communications Manager passes a call to the PSTN, it relies on overlap sending in the PSTN to determine how many digits to collect and where to route the call. Check this check box for each route pattern that you consider to be assigned to a gateway or route list that routes the calls to a PSTN that supports overlap sending.  
  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, the system disables the Allow Overlap Sending check box. |
<p>| Urgent Priority | If the dial plan contains overlapping route patterns, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if dialing a sequence of digits to choose a current match is possible). Check this check box to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Forced Authorization Code</td>
<td>If you want to use forced authorization codes with this route pattern, check this check box. The FAC feature does not support overlap sending because the Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the Allow Overlap Sending check box, the system disables the Require Forced Authorization Code check box.</td>
</tr>
</tbody>
</table>
| Authorization Level      | Enter the authorization level for the route pattern. The number that you specify in this field determines the minimum authorization level that is needed to successfully route a call through this route pattern.  
**Tip** To activate the authorization code, you must check the Require Forced Authorization Code. If you do not check the check box, a message displays when you insert the route pattern that indicates that the authorization code cannot be activated. To activate the code, click Cancel, check the Require Forced Authorization Code check box, and click Insert. To activate the code at a later time, click OK. |
| Require Client Matter Code | If you want to use client matter codes with this route pattern, check this check box. The CMC feature does not support overlap sending because the Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the Allow Overlap Sending check box, the Require Client Matter Code check box become disabled. |

**Calling Party Transformations**

| Use Calling Party's External Phone Number Mask | Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.  
**Note** The calling party transformation settings that are assigned to the route groups in a route list override any calling party transformation settings that are assigned to a route pattern that is associated with that route list. |
| Calling Party Transform Mask | Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9; the wildcard characters X, 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 topics related to calling party number transformation settings in the *Cisco Unified Communications Manager System Guide* for more information. |
| Prefix Digits (Outgoing Calls) | Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the National Numbering Plan 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. |
<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 route 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.</td>
</tr>
<tr>
<td>Calling Name Presentation</td>
<td>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 route 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.</td>
</tr>
</tbody>
</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 Unified Communications Manager—The Cisco Unified Communications Manager sets the directory number type.  
  - Unknown—Use 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. |
### Calling Party Numbering Plan

Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non national type number.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—Use when the dialing plan is unknown.

### Connected Party Transformations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 route 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. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
</tbody>
</table>
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 route 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 topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide.

Formore informations about this field, see topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 route 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 topics related to connected party presentation and restriction settings in the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>

Called Party Transformations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard Digits</td>
<td>From the Discard Digits drop-down list box, choose the discard digits instructions that you want to associate with this route pattern. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. See topics related to discard digits instructions in the Cisco Unified Communications Manager System Guide for more information on discard instructions for the North American Numbering Plan. Note The called party transformation settings that are assigned to the route groups in a route list override any called party transformation settings that are assigned to a route pattern that is associated with that route list.</td>
</tr>
<tr>
<td>Called Party Transform Mask</td>
<td>Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If the field is blank, no transformation takes place. Cisco Unified Communications Manager sends the dialed digits exactly as dialed.</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls)</td>
<td>Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries for the National Numbering Plan 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>
### Field

**Called Party Number Type**

Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national type numbering plan.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Use when the Cisco Unified Communications Manager sets the directory number type.
- **Unknown**—Use 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.

---

**Called Party Numbering Plan**

Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non-national type number.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—Use when the dialing plan is unknown.

---

**ISDN Network-Specific Facilities Information Element**

**Network Service Protocol**

From the Network Service Protocol drop-down list box, choose the PRI protocol that matches the protocol of the terminating gateway.
Enter the appropriate carrier identification code (0, 3, or 4 digits) in the Carrier Identification Code field. Carrier identification codes allow customers to reach the services of interexchange carriers.

The following list shows examples of commonly used carrier identification codes:

- ATT—0288
- Sprint—0333
- WorldCom/MCI—0222

For a complete list of NANP carrier identification codes, visit the NANPA website.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Carrier Identification Code | Enter the appropriate carrier identification code (0, 3, or 4 digits) in the Carrier Identification Code field. Carrier identification codes allow customers to reach the services of interexchange carriers. The following list shows examples of commonly used carrier identification codes:  
  • ATT—0288  
  • Sprint—0333  
  • WorldCom/MCI—0222  
  For a complete list of NANP carrier identification codes, visit the NANPA website. |
| Network Service | Choose the appropriate network service. The values vary depending on the network service protocol that you choose from the Network Service Protocol field. |
| Service Parameter Name | This field displays the service parameter name that is associated with the chosen network service. If no service parameter exists for the network service, the field displays <Not Exist>. |
| Service Parameter Value | Enter the appropriate service parameter value. Valid entries include the digits 0 through 9. If a service parameter does not exist for the network service, Cisco Unified Communications Manager Administration disables this field. |

**Related Topics**

- About route filter setup, on page 169
- Synchronize route list settings with route groups, on page 188
- Route pattern setup, on page 189
- Search for partition, on page 244
Line group setup

This chapter provides information to add or delete a line group or to add directory numbers to or to remove directory numbers from a line group.

For additional information, see topics related to understanding route plans in the Cisco Unified Communications Manager System Guide.

- About line group setup, page 201
- Line group deletion, page 202
- Line group settings, page 202
- Add members to line group, page 207
- Remove members from line group, page 207

About line group setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Route/Hunt > Line Group menu path to configure line groups.

A line group allows you to designate the order in which directory numbers are chosen. Cisco Unified Communications Manager distributes a call to idle or available members of a line group based on a call distribution algorithm and on the Ring No Answer Reversion (RNAR) Timeout setting.

---

**Note**

Users cannot pick up calls to a DN that belongs to a line group by using the Directed Call Pickup feature.

---

**Tip**

Although you can configure an empty line group with no members (directory numbers), Cisco Unified Communications Manager does not support this configuration for routing calls. If the line group contains no members, the hunt list stops hunting when the call gets routed to the empty line group. To avoid this situation, make sure that you configure at least one member in the line group.
**Line group configuration tips**

You must define one or more directory numbers before configuring a line group.

After you configure or update a line group, you can add or remove members from that line group.

**Related Topics**

- Add members to line group, on page 207
- Remove members from line group, on page 207

**Line group deletion**

You cannot delete a line group that one or more route/hunt lists references. To find out which hunt lists are using the line group, in the Line Group Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a line group that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a line group that is currently in use, you must perform the following task:

- Remove the line group from all hunt lists to which it belongs before deleting the line group.

**Tip**

To delete line groups and hunt pilots; first, delete the hunt pilot; second, delete the hunt list; and finally, delete the line group.

**Related Topics**

- Remove route groups from route list, on page 187
- Access dependency records, on page 874

**Line group settings**

The following table describes the line group settings.

*Table 36: Line group settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Group Information</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Line Group Name            | Enter a name for this line group. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that each line group name is unique to the route plan. 

Timesaver  
Use concise and descriptive names for your line groups. The CompanynameLocationGroup format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a line group. For example, CiscoDallasAA1 identifies a Cisco Access Analog line group for the Cisco office in Dallas. |
| RNA Reversion Timeout      | Enter a time, in seconds, after which Cisco Unified CM will distribute a call to the next available or idle member of this line group or to the next line group if the call is not answered and if the first hunt option, Try next member; then, try next group in Hunt List, is chosen. The RNA Reversion Timeout applies at the line-group level to all members. |
| Distribution Algorithm    | Choose a distribution algorithm, which applies at the line-group level, from the options in the drop-down list box:  

- **Top Down**—If you choose this distribution algorithm, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member.  
- **Circular**—If you choose this distribution algorithm, Cisco Unified CM distributes a call to idle or available members starting from the \( (n+1) \)th member of a route group, where the \( n \)th member is the next sequential member in the list who is either idle or busy but not “down.” If the \( n \)th member is the last member of a route group, Cisco Unified CM distributes a call starting from the top of the route group.  
- **Longest Idle Time**—If you choose this distribution algorithm, Cisco Unified CM only distributes a call to idle members, starting from the longest idle member to the least idle member of a line group.  
- **Broadcast**—If you choose this distribution algorithm, Cisco Unified CM distributes a call to all idle or available members of a line group simultaneously. See the Note in the description of the Selected DN/Route Partition field for additional limitations in using the Broadcast distribution algorithm.  

The default value specifies Longest Idle Time. |
| Hunt Options               |                                                                                                                                     |
For a given distribution algorithm, choose a hunt option for Cisco Unified CM to use if a call is distributed to a member of a line group that does not answer. This option gets applied at the member level. Choose from the options in the drop-down list box:

- **Try next member; then, try next group in Hunt List**—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified CM then tries the next line group in a hunt list.

- **Try next member, but do not go to next group**—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CM stops trying upon reaching the last member of the current line group.

- **Skip remaining members, and go directly to next group**—If you choose this hunt option, Cisco Unified CM skips the remaining members of this line group when the RNA reversion timeout value elapses for the first member. Cisco Unified CM then proceeds directly to the next line group in a hunt list.

- **Stop hunting**—If you choose this hunt option, Cisco Unified CM stops hunting after trying to distribute a call to the first member of this line group and the member does not answer the call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No Answer</strong></td>
<td>For a given distribution algorithm, choose a hunt option for Cisco Unified CM to use if a call is distributed to a member of a line group that does not answer. This option gets applied at the member level. Choose from the options in the drop-down list box:</td>
</tr>
<tr>
<td></td>
<td><strong>Try next member; then, try next group in Hunt List</strong>—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified CM then tries the next line group in a hunt list.</td>
</tr>
<tr>
<td></td>
<td><strong>Try next member, but do not go to next group</strong>—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CM stops trying upon reaching the last member of the current line group.</td>
</tr>
<tr>
<td></td>
<td><strong>Skip remaining members, and go directly to next group</strong>—If you choose this hunt option, Cisco Unified CM skips the remaining members of this line group when the RNA reversion timeout value elapses for the first member. Cisco Unified CM then proceeds directly to the next line group in a hunt list.</td>
</tr>
<tr>
<td></td>
<td><strong>Stop hunting</strong>—If you choose this hunt option, Cisco Unified CM stops hunting after trying to distribute a call to the first member of this line group and the member does not answer the call.</td>
</tr>
<tr>
<td><strong>Automatically Logout</strong></td>
<td>If this check box is checked, line members will be logged off the hunt list automatically. Line members can log back in using the &quot;HLOG&quot; softkey or PLK.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Busy</td>
<td>For a given distribution algorithm, choose a hunt option for Cisco Unified CM to use if a call is distributed to a member of a line group that is busy. Choose from the options in the drop-down list box:&lt;br&gt;• Try next member; then, try next group in Hunt List—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified CM then tries the next line group in a hunt list.&lt;br&gt;• Try next member, but do not go to next group—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CM stops trying upon reaching the last member of the current line group.&lt;br&gt;• Skip remaining members, and go directly to next group—If you choose this hunt option, Cisco Unified CM skips the remaining members of this line group upon encountering a busy member. Cisco Unified CM proceeds directly to the next line group in a hunt list.&lt;br&gt;• Stop hunting—If you choose this hunt option, Cisco Unified CM stops hunting after trying to distribute a call to the first busy member of this line group.</td>
</tr>
<tr>
<td>Not Available</td>
<td>For a given distribution algorithm, choose a hunt option for Cisco Unified CM to use if a call is distributed to a member of a line group that is not available. The Not Available condition occurs when none of the phones that are associated with the DN in question is registered. Not Available also occurs when extension mobility is in use and the DN/user is not logged in. Choose from the options in the drop-down list box:&lt;br&gt;• Try next member; then, try next group in Hunt List—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. If unsuccessful, Cisco Unified Communications Manager then tries the next line group in a hunt list.&lt;br&gt;• Try next member, but do not go to next group—If you choose this hunt option, Cisco Unified CM distributes a call to idle or available members starting from the first idle or available member of a line group to the last idle or available member. Cisco Unified CM stops trying upon reaching the last member of the current line group.&lt;br&gt;• Skip remaining members, and go directly to next group—If you choose this hunt option, Cisco Unified CM skips the remaining members of this line group upon encountering the first unavailable member. Cisco Unified CM proceeds directly to the next line group in a hunt list.&lt;br&gt;• Stop hunting—If you choose this hunt option, Cisco Unified CM stops hunting after trying to distribute a call to the first unavailable member of this line group.</td>
</tr>
</tbody>
</table>
### Field Description

**Line Group Member Information**

**Find Directory Numbers to Add to Line Group**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition</td>
<td>Choose a route partition for this line group from the drop-down list box. The default value specifies &lt;None&gt;. If you click Find, the Available DN/Route Partition list box displays all DNs that belong to the chosen partition.</td>
</tr>
<tr>
<td>Directory Number</td>
<td>Enter the character(s) that are found in the directory number that you are seeking and click the Find button. Directory numbers that match the character(s) that you entered display in the Available DN/Route Partition box.</td>
</tr>
<tr>
<td>Available DN/Route</td>
<td>Choose a directory number in the Available DN/Route Partition list box and add it to the Selected DN/Route Partition list box by clicking Add to Line Group.</td>
</tr>
<tr>
<td>Partition</td>
<td></td>
</tr>
<tr>
<td>Current Line Group Members</td>
<td></td>
</tr>
<tr>
<td>Selected DN/Route</td>
<td>To change the priority of a directory number, choose a directory number in the Selected DN/Route Partition list box. Move the directory number up or down in the list by clicking the arrows on the right side of the list box.</td>
</tr>
<tr>
<td>Partition</td>
<td>To reverse the priority order of the directory numbers in the Selected DN/Route Partition list box, click Reverse Order of Selected DNs/Route Partitions.</td>
</tr>
<tr>
<td></td>
<td>For more information about the order of directory numbers in a line group, see topics related to route plans in the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
</tbody>
</table>

**Note** Do not put DNs that are shared lines in a line group that uses the Broadcast distribution algorithm. Cisco Unified CM cannot display all DNs that are shared lines on devices where the DNs are configured as shared lines if the DNs are members of a line group that uses the Broadcast distribution algorithm.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removed DN/Route</td>
<td>Choose a directory number in the Selected DN/Route Partition list box and add it to the Removed DN/Route Partition list box by clicking the down arrow between the two list boxes.</td>
</tr>
<tr>
<td>Partition</td>
<td></td>
</tr>
<tr>
<td>Directory Numbers</td>
<td></td>
</tr>
<tr>
<td>(list of DNs that currently belong to this line group)</td>
<td>Click a directory number in this list to go to the Directory Number Configuration window for the specified directory number.</td>
</tr>
</tbody>
</table>

**Note** When you are adding a new line group, this list does not display until you save the line group.

**Related Topics**

*Line group setup, on page 201*
Add members to line group

You can add members to a new line group or to an existing line group. The following procedure describes adding a member to an existing line group.

**Before You Begin**

You must define one or more directory numbers before performing this procedure.

**Procedure**

1. Choose **Call Routing > Route/Hunt > Line Group**.
2. Locate the line group to which you want to add a member.
3. If you need to locate a directory number, choose a route partition from the Partition drop-down list box, enter a search string in the Directory Number Contains field, and click Find. To find all directory numbers that belong to a partition, leave the Directory Number Contains field blank and click Find. A list of matching directory numbers displays in the Available DN/Route Partition list box.
4. In the Available DN/Route Partition list box, choose a directory number to add and click Add to Line Group to move it to the Selected DN/Route Partition list box. Repeat this step for each member that you want to add to this line group.
5. In the Selected DN/Route Partition list box, choose the order in which the new directory number(s) is to be accessed in this line group. To change the order, click a directory number and use the Up and Down arrows to the right of the list box to change the order of directory numbers.
6. Click Save to add the new directory numbers and to update the directory number order for this line group.

**Related Topics**

- Line group setup, on page 201

Remove members from line group

You can remove members from a new line group or from an existing line group. The following procedure describes removing a directory number from an existing line group.

**Procedure**

1. Choose **Call Routing > Route/Hunt > Line Group**.
2. Locate the line group from which you want to remove a directory number.
3. In the Selected DN/Route Partition list box, choose a directory number to be deleted and click the down arrow below the list box to move the directory number to the Removed DN/Route Partition list box. Repeat this step for each member that you want to remove from this line group.
4. To remove the members, click Save.
Related Topics

Line group setup, on page 201
CHAPTER 36

Hunt list setup

The following chapter provides information to add or remove hunt lists or to add, remove, or change the order of line groups in a hunt list, or synchronize configuration changes with affected line groups.

For additional information, see topics related to understanding route plans in the Cisco Unified Communications Manager System Guide.

• About Hunt List configuration, page 209
• Find hunt lists, page 210
• Add hunt list, page 210
• Add line groups to hunt list, page 211
• Remove line groups from hunt list, page 212
• Change line groups order in hunt list, page 213
• Synchronize hunt list settings with line groups, page 213
• Delete hunt list, page 214

About Hunt List configuration

A Hunt List lists a set of Line groups in a specific order. A hunt list then associates with one or more hunt pilots and determines the order in which those line groups are accessed. The order controls the progress of the search for available directory numbers for incoming calls.

A hunt list comprises a collection of directory numbers as defined by line groups. After Cisco Unified Communications Manager determines a call that is to be routed through a defined hunt list, Cisco Unified Communications Manager finds the first available device on the basis of the order of the line group(s) that a hunt list defines.

Note

The Group Call Pickup feature and Directed Call Pickup feature do not work with hunt lists.

A hunt list can contain only line groups. Each hunt list should have at least one line group. Each line group includes at least one directory number. A single line group can appear in multiple hunt lists.
Find hunt lists

Because you might have several hunt lists in your network, Cisco Unified Communications Manager lets you use specific criteria to locate specific hunt lists. To locate hunt lists, use the following procedure.

Note

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

Procedure

Step 1
Choose Call Routing > Route/Hunt > Hunt List. The Find and List Hunt Lists 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 Find hunt lists, on page 210. To filter or search records

a) From the first drop-down list box, select a search parameter.

b) From the second drop-down list box, select a search pattern.

c) 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.

Related Topics

Hunt list setup, on page 209

Add hunt list

The following procedure describes how to add a hunt list.
Procedure

Step 1 Choose Call Routing > Route/Hunt > Hunt List.

Step 2 Click Add New.

Step 3 In the Name field, enter a name. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure each hunt list name is unique to the route plan.

Warning Use concise and descriptive names for your hunt lists. The Companyname.Location.Calltype format, which usually provides a sufficient level of detail and is short enough, enables you to quickly and easily identify a hunt list. For example, CiscoDallasMetro identifies a hunt list for toll-free, inter-local access transport area (LATA) calls from the Cisco office in Dallas.

Step 4 Enter a description in the Description field.

Step 5 Choose Cisco Unified Communications Manager Group from the drop-down list box.

Note Hunt List registers to the first Cisco Unified Communications Manager in the Cisco Unified Communications Manager Group as primary Cisco Unified Communications Manager.

Note If you choose a Cisco Unified Communications Manager group that has only one Cisco Unified Communications Manager that is configured, you receive the following warning:

Note WARNING! The selected Cisco Unified Communications Manager Group has only one Cisco Unified Communications Manager configured. For the control process to have redundancy protection, please select a Cisco Unified Communications Manager Group with more than one Cisco Unified Communications Manager.

Step 6 If this hunt list is to be used for voice mail, click the For Voice Mail Usage check box.

Step 7 To add this hunt list, click Save.

Note A popup message reminds you that you must add at least one line group to this hunt list for it to accept calls.

The Hunt List window displays the newly added hunt list.

Step 8 The system checks the Enable this Hunt List check box by default for the new hunt list.

If you want to disable this hunt list, uncheck this check box. A popup window explains that calls in progress are not affected, but this hunt list will not accept additional calls.

Step 9 Add at least one line group to the new hunt list.

To add a line group to this list, click Add Line Group and perform Step 3, on page 212 through Step 6, on page 212 of the Add line groups to hunt list, on page 211.

Related Topics

Hunt list setup, on page 209

Add line groups to hunt list

You can add line groups to a new hunt list or to an existing hunt list. Line groups can exist in one or more hunt lists. The following procedure describes adding a line group to an existing hunt list.

Before You Begin

You must build one or more line groups and add a hunt list before performing this procedure.
Procedure

Step 1 Choose Call Routing > Route/Hunt > Hunt List.

Step 2 Locate the hunt list to which you want to add a line group.

Step 3 To add a line group, click Add Line Group.
   The Hunt List Detail Configuration window displays.

Step 4 From the Line Group drop-down list box, choose a line group to add to the hunt list.

Step 5 To add the line group, click Save.
   The line group name displays in the Selected Groups pane.

   Note The added line group also displays in the Hunt List Details pane at the bottom of the Hunt List Configuration window. You can make changes to a line group by clicking on the line group name. Doing so causes the Line Group Configuration window for that line group to display.

Step 6 To add more line groups to this list, click Add Line Group and repeat Step 3, on page 212 through Step 5, on page 212.

Step 7 When you finish adding line groups to the hunt list, click Save.

   Note See topics related to synchronizing a hunt list with affected line groups before deciding whether to proceed to Step 8, on page 212 below.

Step 8 To reset the hunt list, click Reset. When the popup windows display, click Reset.

Related Topics

Hunt list setup, on page 209
Find hunt lists, on page 210
Synchronize hunt list settings with line groups, on page 213

Remove line groups from hunt list

You can remove line groups from a new hunt list or from an existing hunt list. The following procedure describes removing a line group from an existing hunt list.

Procedure

Step 1 Choose Call Routing > Route/Hunt > Hunt List in the menu bar.

Step 2 Locate the hunt list from which you want to remove a line group.

Step 3 From the Selected Groups list, choose a line group name.

   Note To choose multiple line groups from the list, press the Shift key and click the desired line groups.
Step 4  Click the down arrow below the Selected Groups list box to move the chosen line group to the Removed Groups list.

Step 5  To remove the line group, click Save. If you click OK, when the window refreshes, the line group no longer displays in the Selected Groups pane of the hunt list.

Step 6  Click Reset for the changes to take effect. Click Reset and Close in response to the popup window.

Related Topics
   Hunt list setup, on page 209
   Find hunt lists, on page 210

Change line groups order in hunt list

Cisco Unified Communications Manager accesses line groups in the order in which they display in the hunt list. The following procedure allows you to change the access order of line groups.

Procedure

Step 1  Choose Call Routing > Route/Hunt > Hunt List.
Step 2  Locate the hunt list in which you want to change the order of a line group.
Step 3  From the Selected Groups list, choose a line group.
Step 4  To move the line group up or down in the list, select a group; then, click the up or down arrows on the right side of the list box.
Step 5  Click Save.
Step 6  Click Reset for the changes to take effect. Click Reset and Close in response to the popup window.

Related Topics
   Hunt list setup, on page 209
   Find hunt lists, on page 210

Synchronize hunt list settings with line groups

To synchronize line groups with a hunt list that has undergone configuration changes, perform the following procedure, which applies 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 > Route/Hunt > Hunt List.
The Find and List Hunt Lists window displays.
Step 2  Choose the search criteria to use.
Step 3  Click Find.
The window displays a list of hunt lists that match the search criteria.
Step 4  Check the check boxes next to the hunt lists to which you want to synchronize applicable line groups. To choose all hunt lists in the window, check the check box in the matching records title bar.
Step 5  Click Apply Config to Selected.
The Apply Configuration Information dialog displays.
Step 6  Click OK.

Related Topics
- Hunt list setup, on page 209

Delete hunt list

Cisco Unified Communications Manager associates hunt lists with line groups and hunt pilots; however, deletion of line groups and hunt pilots does not occur when the hunt list is deleted. To find out which hunt pilots are using the hunt list, click the Dependency Records link from the Hunt List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

Tip
To delete line groups and hunt pilots, first delete the hunt pilot; second, delete the hunt list; and finally, delete the line group.

The following procedure describes how to delete a hunt list.

Procedure

Step 1  Choose Call Routing > Route/Hunt > Hunt List.
Step 2  Locate the hunt list that you want to delete.
Step 3  Click Delete.
  A dialog box displays to warn you that you cannot undo the deletion of a hunt list.
Step 4  To delete the hunt list, click OK or to cancel the action, click Cancel.
  Caution  You cannot delete a hunt list if it is associated with one or more hunt pilots.

Related Topics
- Hunt list setup, on page 209
- Find hunt lists, on page 210
- Access dependency records, on page 874
Hunt pilot setup

This chapter provides information to add, configure, or delete a hunt pilot. For additional information about understanding route plans, wildcards and special characters in route patterns and hunt pilots, see the Cisco Unified Communications Manager System Guide.

- About hunt pilot setup, page 215
- Hunt pilot settings, page 216

About hunt pilot setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Route/Hunt > Hunt Pilot menu path to configure hunt pilots.

A hunt pilot comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

See topics related to understanding route plans in the Cisco Unified Communications Manager System Guide for more detailed hunt pilot information.

Call Queuing

The Call Queuing feature provides an enhanced capability for handling incoming calls to a hunt pilot number. For detailed information on the Call Queuing feature, see “Call Queuing”, in Cisco Unified Communications Manager Features and Services Guide.

Hunt pilot configuration tips

Before you begin, ensure that the following items are configured in Cisco Unified Communications Manager:

- Hunt list
- Partition (unless you are using <None>)
- Route filter (unless you are using <None>)
Assigning 8XXX to a hunt pilot causes hunting through all directory numbers 8000 to 8999. Similarly, 82XX hunts through directory numbers 8200 to 8299. See topics related to special characters and settings in the Cisco Unified Communications Manager System Guide for more information about wildcards.

Timesaver

After you choose a hunt list from the Hunt List drop-down list box, you can use the (Edit) link that displays next to the Hunt List field to take you to the Hunt List Configuration window for the hunt list that you choose. Use the Hunt List Configuration window to see the line group(s) that are included in that hunt list.

Note

Hunt pilot settings

The following table describes the available fields in the Hunt Pilot Configuration window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Definition</td>
<td>Enter the hunt pilot, including numbers and wildcards (do not use spaces); for example, for NANNP, 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 +.</td>
</tr>
<tr>
<td>Note</td>
<td>Ensure that the directory hunt pilot, which uses the chosen partition, route filter, and numbering plan combination, is unique. Check the hunt pilot, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report.</td>
</tr>
<tr>
<td>Note</td>
<td>• See topics related to wildcards and special characters in route patterns and hunt pilots in the Cisco Unified Communications Manager System Guide for more information about wildcards.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Route Partition       | If you want to use a partition to restrict access to the hunt pilot, choose the desired partition from the drop-down list box. If you do not want to restrict access to the hunt pilot, 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, then find and choose a partition name.  
**Note** To set the maximum list box items, choose System > Enterprise Parameters and choose Unified CMAadmin Parameters.  
**Note** Make sure that the combination of hunt pilot, route filter, and partition is unique within the Cisco Unified CM cluster. |
| Description           | Enter a description of the hunt pilot. 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.                                                                                                                      |
| Route Filter          | If your hunt pilot includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns.  
The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.  
You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name.  
**Note** To set the maximum list box items, choose System > Enterprise Parameters and choose Unified CMAadmin Parameters. |
| MLPP Precedence       | Choose an MLPP precedence setting for this hunt pilot from the drop-down list box:  
• Executive Override—Highest precedence setting for MLPP calls.  
• Flash Override—Second highest precedence setting for MLPP calls.  
• Flash—Third highest precedence setting for MLPP calls.  
• Immediate—Fourth highest precedence setting for MLPP calls.  
• Priority—Fifth highest precedence setting for MLPP calls.  
• Routine—Lowest precedence setting for MLPP calls.  
• Default—Does not override the incoming precedence level but rather lets it pass unchanged.  
**Note** See topics related to multilevel precedence and preemption in the Cisco Unified Communications Manager Features and Services Guide for more information. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hunt List</td>
<td>Choose the hunt list for which you are adding a huntpilot from the drop-down list box. After you choose a hunt list, click the Edit link to the right to edit the hunt list.</td>
</tr>
<tr>
<td>Alerting Name</td>
<td>Enter an alerting name for the huntpilot in UNICODE format. This name gets displayed on phones that the huntpilot dials when it receives an incoming call, along with calling party information. The phone users can use this information to answer the call accordingly. This name also gets displayed on the calling phone. If you do not enter a name, the huntpilot DN displays on the phones.</td>
</tr>
<tr>
<td>ASCII Alerting Name</td>
<td>Enter an alerting name for the huntpilot in ASCII format. This name gets displayed on phones that the huntpilot dials when it receives an incoming call, along with calling party information. The phone users can use this information to answer the call accordingly. This name also gets displayed on the calling phone. If you do not enter a name, the huntpilot DN displays on the phones.</td>
</tr>
</tbody>
</table>
| Route Option      | The Route Option designation indicates whether you want this huntpilot 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. If you choose the Block this pattern radio button, you must choose the reason for which you want this huntpilot to block calls. Choose a value from the drop-down list box:  
  • No Error  
  • Unallocated Number  
  • Call Rejected  
  • Number Changed  
  • Invalid Number Format  
  • Precedence Level Exceeded |
| Provide Outside Dial Tone | Provide Outside Dial Tone indicates that Cisco Unified CM routes the calls off the local network. Check this check box for each huntpilot that routes the call off the local network and provides outside dial tone to the calling device. To route the call in the network, leave the check box unchecked. |
| Urgent Priority   | If the dial plan contains overlapping hunt lists, Cisco Unified CM would 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 CM must route a call immediately. |

Hunt Forward Settings
When the call that is distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose from the following options:

- **Use Personal Preferences**—Use this check box to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to this hunt pilot.
  
  The CFNC setting specifies a call forwarding reason that you administer in the Directory Number Configuration window. Calls get diverted based on the value in the directory number Coverage/Destination field when a call to the directory number first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding.

  **Note** When this check box is checked, Cisco Unified CM ignores the settings in the Destination box and Calling Search Space.

  - **Destination**—This setting indicates the directory number to which calls are forwarded.
  
  - **Calling Search Space**—This setting applies to all devices that are using this directory number.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Forward Hunt No Answer | When the call that is distributed through the hunt list is not answered in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose from the following options:  
  
  - **Use Personal Preferences**—Use this check box to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to this hunt pilot.
    
    The CFNC setting specifies a call forwarding reason that you administer in the Directory Number Configuration window. Calls get diverted based on the value in the directory number Coverage/Destination field when a call to the directory number first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding.
  
  **Note** When this check box is checked, Cisco Unified CM ignores the settings in the Destination box and Calling Search Space.
  
  - **Destination**—This setting indicates the directory number to which calls are forwarded.
  
  - **Calling Search Space**—This setting applies to all devices that are using this directory number. |
| Forward Hunt Busy | When the call that is distributed through the hunt list is busy in a specific period of time, this field specifies the destination to which the call gets forwarded. Choose from the following options:  
  
  - **Use Personal Preferences**—Use this check box to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to this hunt pilot.
    
    The CFNC setting specifies a call forwarding reason that you administer in the Directory Number Configuration window. Calls get diverted based on the value in the directory number Coverage/Destination field when a call to the directory number first diverts to coverage, and coverage either exhausts or times out, and the associated hunt pilot for coverage specifies Use Personal Preferences for its final forwarding.
  
  **Note** When this check box is checked, Cisco Unified CM ignores the settings in the Destination box and Calling Search Space.
  
  - **Destination**—This setting indicates the directory number to which calls are forwarded.
  
  - **Calling Search Space**—This setting applies to all devices that are using this directory number. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Hunt Timer</td>
<td>Enter a value (in seconds) that specifies the maximum time for hunting. Valid values specify 1 to 3600. The default value specifies 1800 seconds (30 minutes). This timer cancels if either a hunt member answers the call or if the hunt list gets exhausted before the timer expires. If you do not specify a value for this timer, hunting continues until a hunt member answers or hunting exhausts. If neither event takes place, hunting continues for 30 minutes, after which the call gets taken for final treatment. <strong>Note</strong> If hunting exceeds the number of hops that the Forward Maximum Hop Count service parameter specifies, hunting expires before the 30-minute maximum hunt timer value, and the caller receives a reorder tone. In addition, Cisco Unified CM only uses the configuration for the Maximum Hunt Timer setting if you configure the Hunt Forward settings in the Hunt Pilot Configuration window.</td>
</tr>
<tr>
<td>Park Monitoring</td>
<td></td>
</tr>
<tr>
<td>Park Monitoring Forward No Retrieve Destination</td>
<td>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) to forward the parked call when the service parameter Park Monitoring Forward No Retrieve Timer expires. If the parameter value of the Hunt Pilot Park Monitoring Forward No Retrieve Destination parameter 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. Specify the following values:  • Destination—This setting specifies the directory number to which a parked call is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination.  • Calling Search Space—A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call.</td>
</tr>
<tr>
<td>Calling Party Transformations</td>
<td></td>
</tr>
<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. You may also configure an External Phone Number Mask on all phone devices. <strong>Note</strong> The calling party transformation settings that are assigned to the line groups in a hunt list override any calling party transformation settings that are assigned to a hunt pilot that is associated with that hunt list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Calling Party Transform Mask</td>
<td>Enter a transformation mask value. Valid entries include the digits 0 through 9, the wildcard character X, 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 topics related to calling party number transformations settings in the <em>Cisco Unified Communications Manager Features and Services Guide</em> for more information.</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls)</td>
<td>Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9; the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. <strong>Note</strong> The appended prefix digit does not affect which directory numbers route to the assigned device.</td>
</tr>
<tr>
<td>Calling Line ID Presentation</td>
<td>Cisco Unified CM 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 CM to allow or restrict the display of the calling party phone number on the called party phone display for this hunt pilot. Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified CM to allow the display of the calling number. Choose Restricted if you want Cisco Unified CM to block the display of the calling number. For more information about this field, see topics related to calling party number transformations settings in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Display Line Group Member DN as Connected Party</td>
<td>Check this check box to display the directory number of the answering phone as the connected party when a call is routed through a hunt list. Uncheck this check box to display the hunt pilot number as the connected party when a call is routed through a hunt list.</td>
</tr>
<tr>
<td>Calling Name Presentation</td>
<td>Cisco Unified CM 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 CM to allow or restrict the display of the calling party name on the called party phone display for this hunt pilot. Choose Default if you do not want to change calling name presentation. Choose Allowed if you want Cisco Unified CM to display the calling name information. Choose Restricted if you want Cisco Unified CM to block the display of the calling name information. For more information about this field, see topics related to calling party number transformations settings in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>

### Calling Party Number Type

Choose the format for the number type in calling party directory numbers. Cisco Unified CM 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 CM 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 Unified Communications Manager**—The Cisco Unified Communications Manager sets the directory number type.
- **Unknown**—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.

### Calling Party Numbering Plan

Choose the format for the numbering plan in calling party directory numbers. Cisco Unified CM sets the calling DN numbering plan. 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 CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—Use when the dialing plan is unknown.

### Connected Party Transformations
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 CM to allow or restrict the display of the connected party phone number on the calling party phone display for this hunt pilot. 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 CM to block the display of the connected party phone number. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see topics related to connected party presentation and restriction settings in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Connected Name Presentation</td>
<td>Cisco Unified CM 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 CM to allow or restrict the display of the connected party name on the calling party phone display for this hunt pilot. 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 CM to block the display of the connected party name. For more information about this field, see topics related to connected party presentation and restriction settings in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Called Party Transformations</td>
<td>From the Discard Digits drop-down list box, choose the discard digits instructions that you want to associate with this hunt pilot. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box. See topics related to discard digits instructions in the <em>Cisco Unified Communications Manager System Guide</em> for more information on discard instructions for the North American Numbering Plan. <strong>Note</strong> The called party transformation settings that are assigned to the line groups in a hunt list override any called party transformation settings that are assigned to a hunt pilot that is associated with that hunt list. Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If the field is blank, no transformation takes place. Cisco Unified CM sends the dialed digits exactly as dialed.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls)</td>
<td>Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9; the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. <strong>Note</strong> The appended prefix digit does not affect which directory numbers route to the assigned device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Called Party Number Type</strong></th>
<th>Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Use when the dialing plan is unknown.</td>
</tr>
<tr>
<td></td>
<td>• National—Use when you are dialing within the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• International—Use when you are dialing outside the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Called Party Numbering Plan</strong></th>
<th>Choose the format for the numbering plan in called party directory numbers. Cisco Unified CM sets the called DN numbering plan. 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 CM does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number. Choose one of the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.</td>
</tr>
<tr>
<td></td>
<td>• ISDN—Use when you are dialing outside the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• National Standard—Use when you are dialing within the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• Private—Use when you are dialing within a private network.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Use when the dialing plan is unknown.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
AAR Group Settings |  
AAR Group | Choose an Automated Alternate Routing (AAR) group from the drop-down list box.
External Number Mask | Enter an external number mask value for the hunt pilot. Cisco Unified CM uses this mask to format calling line identification for external (outbound) calls. When AAR initiates a reroute, the system applies this external number mask to the hunt pilot number to form a fully qualified DN of the called party, which allows AAR to reroute properly in out-of-bandwidth conditions.

### Related Topics
- About route filter setup, on page 169
- Hunt pilot setup, on page 215
- Partition setup, on page 241
- Search for partition, on page 244
CHAPTER 38

SIP route pattern setup

This chapter provides information about SIP Route Pattern configuration.

- About SIP route pattern setup, page 227
- SIP route pattern deletion, page 228
- SIP route pattern settings, page 228

About SIP route pattern setup

In Cisco Unified Communications Manager Administration, use the Call Routing > SIP Route Pattern menu path to configure SIP route patterns.

Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls.

The domain name or IP address provides the basis for routing. The administrator can add domains, IP addresses, and IP network (subnet) addresses and associate them to SIP trunks (only). This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.

Because no default SIP route patterns exist in Cisco Unified Communications Manager, the administrator must set them up.

Domain name examples: cisco.com, my-pc.cisco.com, *.com, rtp-ccm[1-5].cisco.com

Valid characters for domain names: [.,- , 0-9, A-Z, a-z, *, and ].

IPv4 address examples: 172.18.201.119 or 172.18.201.119/32 (explicit IP host address); 172.18.0.0/16 (IP subnet); 172.18.201.18/21 (IP subnet).
Valid characters for IP addresses: 0-9, ., and /

SIP route patterns configuration tips
Before you begin, ensure at least one SIP Profile and SIP trunk are configured before you can configure a SIP route pattern.

Related Topics
Set up trunk, on page 646

SIP route pattern deletion
If the SIP route pattern is not in use, Cisco Unified Communications Manager deletes it. If it is in use, a message displays.

SIP route pattern settings
The following table describes the SIP route pattern settings.

Table 38: SIP route pattern settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Definition</td>
<td>(Required) From the drop-down list, choose either Domain Routing or IPAddress Routing.</td>
</tr>
<tr>
<td>Pattern Usage</td>
<td>(Required) Enter the domain, sub-domain, IPv4 address, or IP subnetwork address. For Domain Routing pattern usage, enter a domain name IPv4 Pattern field that can resolve to an IPv4 address. The domain name can contain the following characters: [.,,,0-9,A-Z,a-z,*], and ]. For IP Address Routing pattern usage, enter an IPv4 address the IPv4 Pattern field that follows the format X.X.X.X, where X represents a number between 0 and 255. For the IP subnetwork address, in Classless Inter-Domain Routing (CIDR) notation, X.X.X.X/Y; where Y is the network prefix that denotes the number of bits in the address that will be the network address.</td>
</tr>
<tr>
<td>IPv4 Pattern</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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. If the SIP trunk supports IPv6 or both IPv4 and IPv6 (dual-stack mode), configure the IPv4 Pattern in addition to the IPv6 Pattern.</td>
</tr>
<tr>
<td>Description</td>
<td>For this optional entry, enter a description of the SIP Route Pattern. 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>
<tr>
<td>Route Partition</td>
<td>If you want to use a partition to restrict access to the SIP route pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the SIP route pattern, choose &lt;None&gt; 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 than 250 partitions are specified by using the Max List Box Items enterprise parameter, the Find button displays next to the drop-down list box. Click the Find button to display the Select Partition window. Enter a partial partition name in the List items where Name contains field. Click the desired partition name in the list of partitions that displays in the Select item to use box and click Add Selected.</td>
</tr>
<tr>
<td></td>
<td>To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters. Make sure that the combination of SIP route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>SIP Trunk/Route List</td>
<td>(Required) From the drop-down list choose the SIP trunk or route list to which the SIP route pattern should be associated. Click Edit to open the trunk or route list in the Trunk or Route List Configuration window. URI dialing is available over SIP trunks only. If you are using URI dialing and you select a route list from this drop-down list box, the route list must contain route groups with SIP trunks only.</td>
</tr>
<tr>
<td>Block Pattern</td>
<td>If you do not want this pattern to be used for routing calls, click the Block Pattern check box.</td>
</tr>
</tbody>
</table>

**Calling Party Transformations**

**Use Calling Party's External Phone Mask**

Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls. You may also configure an External Phone Number Mask on all phone devices.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Party Transformation Mask</td>
<td>Enter a transformation mask value. Valid entries include the digits 0 through 9 and the wildcard characters X, asterisk (*), and octothorpe (#). If this field is blank and the preceding field is not checked, no calling party transformation takes place. See topics related to calling party number transformations settings in the <em>Cisco Unified Communications Manager System Guide</em> for more information.</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls)</td>
<td>Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9 and the wildcard characters asterisk (*) and octothorpe (#). Note: The appended prefix digit does not affect which directory numbers route to the assigned device.</td>
</tr>
<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 SIP route 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 topics related to calling party number transformations settings in the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>Calling Line Name Presentation</td>
<td>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 SIP route 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 topics related to calling party number transformations settings in the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>Connected Party Transformations</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Connected Line ID Presentation | 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 SIP route 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.  
If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed.  
For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide*. |
| Connected Line Name Presentation | 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 SIP route 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 topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide*. |

**Related Topics**

- SIP route pattern setup, on page 227
- Partition setup, on page 241
SIP route pattern settings
CHAPTER 39

Time period setup

This chapter provides information to add, update, copy, or delete a time period.
For additional information, see topics related to time-of-day routing in the Cisco Unified Communications Manager System Guide.

- About time period setup, page 233
- Time period deletions, page 233
- Time period settings, page 234

About time period setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Class of Control > Time Period menu path to configure time periods.

A time period comprises a time range that is defined by a start time and end time. Time periods also specify a repetition interval either as days of the week or a specified date on the yearly calendar. You define time periods and then associate the time periods with time schedules. A particular time period can be associated with multiple time schedules.

You then associate time schedules with partitions to set up time-of-day call routing. For more detailed information on time periods and time schedules, see topics related to time-of-day routing in the Cisco Unified Communications Manager System Guide.

Time period deletions

You cannot delete time periods that time schedules are using. To find out which time schedules or other items are using the time period, choose Dependency Records from the Related Links drop-down list box that is on the Time Period Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a time period that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a time period that is currently in use, you must perform either or both of the following tasks:

- Assign a different time period to any time schedules that are using the time period that you want to delete.
• Delete the time schedules that are using the time period that you want to delete.

**Related Topics**

- About time schedule setup, on page 237
- Time schedule deletions, on page 237
- Access dependency records, on page 874

## Time period settings

The following table describes the time period settings.

**Table 39: Time period settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Period Information</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name in the Time Period 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 time period name is unique to the plan.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Use concise and descriptive names for your time periods. The hours <em>or</em> days format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a time period. For example, office <em>M</em> to <em>F</em> identifies a time period for the business hours of an office from Monday to Friday. Cisco Unified Communications Manager provides the All the time time period. This special, system time period includes all hours, is published to end users, and cannot be deleted; this time period can be copied.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this time period.</td>
</tr>
<tr>
<td>Time Of Day Start</td>
<td>From the drop-down list box, choose the time when this time period starts. The available listed start times comprise 15-minute intervals throughout a 24-hour day. The default value is No Office Hours.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> To start a time period at midnight, choose the 00:00 value.</td>
</tr>
<tr>
<td>Time of Day End</td>
<td>From the drop-down list box, choose the time when this time period ends. The available listed end times comprise 15-minute intervals throughout a 24-hour day. The default value is No Office Hours.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You must choose an End Time that is later than the Start Time that you chose.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> To end a time period at midnight, choose the 24:00 value.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Repeat Every | Click on one of the radio buttons:
  - Week from—If you click on the Week from radio button, use the drop-down list boxes next to from and through to choose the days of the week during which this time period applies. Examples: Choose a from value of Mon(day) and a through value of Fri(day) to define a time period that applies from Monday through Friday. Choose a from value of Sat(ursday) and a through value of Sat(ursday) to define a time period that applies only on Saturdays.
  - Year on—If you click on the Year on radio button, use the drop-down list boxes next to Year on and until to choose the month-and-day combinations of the year during which this time period applies. Example: Choose a Year on value of Jan and 15 and an until value of Mar and 15 to choose the days from January 15 to March 15 during which this time period applies. Choose a Year on value of Jan and 1 and an until value of Jan and 1 to specify January 1st as the only day during which this time period applies.

Clear Repeat | Click this button to clear the previously chosen Repeat Every values from the time period that you are modifying.

**Related Topics**

- Time period setup, on page 233
Time period settings
Time schedule setup

This chapter provides information to find, add, update, copy, or delete a time schedule:
For additional information, see topics related to time-of-day routing in the Cisco Unified Communications Manager System Guide.

• About time schedule setup, page 237
• Time schedule deletions, page 237
• Time schedule settings, page 238

About time schedule setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Class of Control > Time Schedule menu path to configure time schedules.

A time schedule comprises a group of time periods. Time schedules get assigned to partitions. Time schedules determine the partitions where calling devices search when they are attempting to complete a call during a particular time of day. Multiple time schedules can use a single time period.

For more detailed information on time schedules, see topics related to time-of-day routing in the Cisco Unified Communications Manager System Guide.

Time schedule deletions

You cannot delete time schedules that partitions are using. To find out which items are using the time schedule, choose Dependency Records from the Related Links drop-down list box that is on the Time Schedule Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a time schedule that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a time schedule that is currently in use, you must perform either or both of the following tasks:

• Assign a different time schedule to any partitions that are using the time schedule that you want to delete.
• Delete the partitions that are using the time schedule that you want to delete.
Before you delete a time schedule, check carefully to ensure that you are deleting the correct time schedule. You cannot retrieve deleted time schedules. If you accidentally delete a time schedule, you must rebuild it.

Related Topics
About partition setup, on page 241
Access dependency records, on page 874

Time schedule settings

The following table describes the time schedule settings.

Table 40: Time schedule settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Schedule Information</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name in the 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 time schedule name is unique to the plan.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Use concise and descriptive names for your time schedules.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager provides the All the time time schedule. This special, system time schedule includes all days and all hours, is published to end users, and cannot be deleted; this time schedule can be copied.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this time schedule.</td>
</tr>
<tr>
<td>Time Period Information</td>
<td></td>
</tr>
<tr>
<td>Available Time Periods</td>
<td>This field displays after a time schedule has been added.</td>
</tr>
<tr>
<td></td>
<td>Choose a time period in the Available Time Periods list box and add it to the Selected Time Periods list box by clicking the down arrow button between the two list boxes.</td>
</tr>
<tr>
<td></td>
<td>To add a range of time periods at once, click the first time period in the range; then, hold down the Shift key while clicking the last time period in the range. Click the down arrow button between the two list boxes to add the range of time periods.</td>
</tr>
<tr>
<td></td>
<td>To add multiple time periods that are not contiguous, hold down the Control (Ctrl) key while clicking multiple time periods. Click the down arrow button between the two list boxes to add the chosen time periods.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Selected Time Periods</td>
<td>This list box lists the time periods that were selected for this time schedule. To remove a time period from the list of selected time periods, choose the time period to remove and click the up arrow between the two list boxes. To reorder the selected time periods, choose a time period and click the up and down arrows to the right of this list box.</td>
</tr>
<tr>
<td>Note</td>
<td>If multiple time periods get associated to a time schedule and the time periods overlap, time periods with Day of Year settings take precedence over time periods with Day of Week settings.</td>
</tr>
<tr>
<td></td>
<td>Example: If a Time Period configured for January 1st is configured as No Office Hours and another time period is configured for the same day of the week (for example, Sunday to Saturday) as 08:00 to 17:00, the time period for January 1st gets used. In this example, No Office Hours takes precedence.</td>
</tr>
<tr>
<td>Note</td>
<td>Time interval settings take precedence over No Office Hour settings for the same day of the year or day of the week.</td>
</tr>
<tr>
<td></td>
<td>Example: One time period specifies for Saturday as No Office Hours. Another time period specifies Saturday hours of 08:00 to 12:00. In this example, the resulting time interval specifies 08:00 to 12:00 for Saturday.</td>
</tr>
<tr>
<td>Note</td>
<td>If multiple time periods are associated to a time schedule and the time periods overlap, time periods with Day of Week settings take precedence over time periods with Range of Days settings.</td>
</tr>
<tr>
<td></td>
<td>Example: If a Time Period configured for Day of Week (for example, Sunday to Saturday) is configured as No Office Hours and another time period is configured for January 1st until December 31st as 08:00 to 17:00, the time period for Day of Week is used. In this example, No Office Hours takes precedence.</td>
</tr>
</tbody>
</table>
Partition setup

This chapter provides information to find, add, update, or delete route partitions.

For additional information, see topics related to local route groups in the *Cisco Unified Communications Manager Features and Services Guide*.

- About partition setup, page 241
- Partition deletions, page 242
- Partition settings, page 242
- Search for partition, page 244
- Synchronize partition settings with devices, page 244

### About partition setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Class of Control > Partition** menu path to configure partitions.

A 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 and calling search spaces, see the *Cisco Unified Communications Manager System Guide*.

**Partitions configuration tips**

You can configure multiple partitions. To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions at a time; the names and descriptions can have a total of up to 1475 characters. Use a comma (,) to separate the partition name and description on each line. If you do not enter a description, Cisco Unified Communications Manager uses the name as the description.

<table>
<thead>
<tr>
<th>Timesaver</th>
</tr>
</thead>
</table>

Use concise and descriptive names for your partitions. The CompanyNameLocationCalltype format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a partition. For example, CiscoDallasMetroPT identifies a partition for toll-free, inter-local access and transport area (LATA) calls from the Cisco office in Dallas.
If you are updating a partition, click Reset, or use the Apply Config button as described in the procedure to synchronize a partition with affected devices. When you reset devices that are associated with the partition, all calls on affected gateways drop.

**Related Topics**
- Search for partition, on page 244
- Synchronize partition settings with devices, on page 244

### Partition deletions

You cannot delete a 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 partition, choose Dependency Records from the Related Links drop-down list box in the Partition Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. 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 partition to any calling search spaces, devices, or other items that are using the partition that you want to delete.
- Delete the calling search spaces, devices, or other items that are using the partition that you want to delete.

**Caution**

Before initiating a deletion, check carefully to ensure that you are deleting the correct partition. You cannot retrieve deleted partitions. If you accidentally delete a partition, you must rebuild it.

**Related Topics**
- Access dependency records, on page 874

### Partition settings

The following table describes the partition settings.

**Table 41: Partition settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition Information</td>
<td></td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Partition Name, Description)</td>
<td>Enter a name in the partition name and description box. Ensure each partition name is unique to the route plan. Partition names can contain a-z, A-Z and 0-9 characters, as well as spaces, hyphens (-), and underscore characters (_).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The length of the partition names limits the maximum number of partitions that can be added to a calling search space. The calling search space partition limitations table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length.</td>
</tr>
<tr>
<td></td>
<td>Follow the 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 (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), angle brackets (&lt;&gt;), or brackets ([ ]).</td>
</tr>
<tr>
<td></td>
<td>If you do not enter a description, Cisco Unified Communications Manager automatically enters the partition name in this field. Use a new line for each partition and description.</td>
</tr>
</tbody>
</table>

| Time Schedule | From the drop-down list box, choose a time schedule to associate with this partition. The associated time schedule specifies when the partition is available to receive incoming calls. 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 incoming calls to this partition against the specified time schedule. |

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Choose one of the following options to associate a partition with a time zone:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>These options all specify the Time Zone. When an incoming call 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.</td>
</tr>
</tbody>
</table>

The following table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. See topics related to partition name limitations in the *Cisco Unified Communications Manager System Guide* for details about how this maximum number is calculated.

**Table 42: 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>
</tbody>
</table>
### Related Topics

Partition setup, on page 241

### Search for 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 Partition drop-down list box on the Cisco Unified Communications Manager Administration windows where the button appears. Click the Find button to search for the partition that you want.

**Procedure**

**Step 1** Click the Find button next to the Partition drop-down list box.  
The Find and List Partitions window displays.

**Step 2** In the Find partition where field, choose search criteria and enter a partial partition name.

**Step 3** In the list of partitions that displays, click the desired partition name and click OK.

**Related Topics**

Partition setup, on page 241

### Synchronize partition settings with devices

To synchronize devices with a partition that has undergone configuration changes, perform the following procedure, which applies 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 > Class of Control > Partition**.
The Find and List Partitions window displays.

Step 2  Choose the search criteria to use.

Step 3  Click Find.
The window displays a list of partitions that match the search criteria.

Step 4  Click the partition to which you want to synchronize applicable devices. The 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 partition get reset, all calls on affected gateways drop.

Step 8  Click OK.

Related Topics

Partition setup, on page 241
Synchronize partition settings with devices
Calling search space setup

This chapter provides information to find, add, update, copy, or delete a calling search space.

For additional information, see topics related to local route groups in the Cisco Unified Communications Manager Features and Services Guide.

- About calling search space setup, page 247
- Calling search space deletions, page 247
- Calling search space settings, page 248

About calling search space setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Class of Control > Calling Search Space menu path to configure calling search spaces (CSS).

A calling search space comprises an ordered list of route partitions that are typically assigned to devices. 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 the Cisco Unified Communications Manager System Guide.

Calling search space deletions

You cannot delete 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 calling search space, choose the Dependency Records from the Related Links drop-down list box in the 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. If you try to delete a calling search space that is in use, Cisco Unified Communications Manager displays a message. Before deleting a calling search space that is currently in use, you must perform either or both of the following tasks:

- Assign a different calling search space to any devices, lines, or translation patterns that are using the calling search space that you want to delete.
- Delete the devices, lines, or translation patterns that are using the calling search space that you want to delete.
Calling search space settings

The following table describes the calling search space settings.

Table 43: Calling search space settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Search Space Information</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name in the 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. Note Use concise and descriptive names for your 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.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description in the Description field. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Route Partitions for this Calling Search Space</td>
<td></td>
</tr>
</tbody>
</table>
Choose a partition in the Available Partitions list box and add it to the Selected Partitions list box by clicking the arrow button between the two list boxes.

To add a range of partitions at once, click the first partition in the range; then, hold down the Shift key while clicking the last partition in the range. Click the arrow button between the two list boxes to add the range of partitions.

To add multiple partitions that are not contiguous, hold down the Control (Ctrl) key while clicking multiple partitions. Click the arrow button between the two list boxes to add the chosen partitions.

**Note**  
The length of the partition names limits the maximum number of partitions that can be added to a calling search space. The calling search space partition limitations table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Available Partitions | Choose a partition in the Available Partitions list box and add it to the Selected Partitions list box by clicking the arrow button between the two list boxes.  
To add a range of partitions at once, click the first partition in the range; then, hold down the Shift key while clicking the last partition in the range. Click the arrow button between the two list boxes to add the range of partitions.  
To add multiple partitions that are not contiguous, hold down the Control (Ctrl) key while clicking multiple partitions. Click the arrow button between the two list boxes to add the chosen partitions. |
| Selected Partitions | To change the priority of a partition, choose a partition name in the Selected Partitions list box. Move the partition up or down in the list by clicking the arrows on the right side of the list box. |

The following table provides examples of the maximum number of partitions that can be added to a calling search space if partition names are of fixed length. See topics related to partition name limitations in the *Cisco Unified Communications Manager System Guide* for details about how this maximum number is calculated.

**Table 44: 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>

**Related Topics**

Calling search space setup, on page 247
Translation pattern setup

This chapter provides information to add, update, copy, or delete a translation pattern. For additional information, see topics related to understanding route plans in the *Cisco Unified Communications Manager System Guide*.

- About translation pattern setup, page 251
- Translation pattern deletions, page 252
- Translation pattern settings, page 252

About translation pattern setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Translation Pattern** menu path to configure translation patterns.

Cisco Unified Communications Manager uses 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.

**Translation patterns configuration tips**

Configure the following Cisco Unified Communications Manager items before configuring a translation pattern:

- Partition
- Route filter
- Calling search space
- Resource-Priority Namespace Network Domain
Ensure that the 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.

Translation pattern deletions

Check carefully to ensure that you are deleting the correct translation pattern before you initiate this action. You cannot retrieve deleted translation patterns. If you accidentally delete a translation pattern, you must rebuild it.

Translation pattern settings

The following table describes the available fields in the Translation Pattern Configuration window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Definition</td>
<td>Enter the translation pattern, including numbers and wildcards (do not use spaces), in the 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>
</tbody>
</table>

**Note** Ensure that the translation pattern, which uses the chosen 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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition</td>
<td>Choose a partition. If you do not want to assign a partition, choose &lt;None&gt;. If you choose &lt;None&gt;, you must enter a value in the Translation Pattern field. 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, then find and choose a partition name. <strong>Note</strong> To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters. Make sure that the combination of translation pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the translation pattern. 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>
<tr>
<td>Numbering Plan</td>
<td>Choose a numbering plan. If your 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 topics related to wildcards and special characters in route patterns and hunt pilots in the Cisco Unified Communications Manager System Guide, as well as topics related to route filter configuration settings 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. <strong>Note</strong> To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters.</td>
</tr>
</tbody>
</table>
### Translation pattern settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **MLPP Precedence** | Choose an MLPP precedence setting for this translation pattern from the drop-down list box:  
  - Executive Override—Highest precedence setting for MLPP calls.  
  - Flash Override—Second highest precedence setting for MLPP calls.  
  - Flash—Third highest precedence setting for MLPP calls.  
  - Immediate—Fourth highest precedence setting for MLPP calls.  
  - Priority—Fifth highest precedence setting for MLPP calls.  
  - Routine—Lowest precedence setting for MLPP calls.  
  - Default—Does not override the incoming precedence level but rather lets it pass unchanged.  
  
  **Note** | See topics related to multilevel precedence and preemption in the *Cisco Unified Communications Manager Features and Services Guide* for more information. |
| **Resource-Priority Namespace Network Domain** | Choose an already configured Resource-Priority Namespace Network Domain from the drop-down list box. |
| **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 can 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.  
  
  If the route pattern points to a SIP trunk supporting G.711, then specify Data or Hotline as the Route Class. |
From the drop-down list box, choose the calling search space for which you are adding a translation pattern, if necessary.

You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 a calling search space name.

**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>Calling Search Space</td>
<td>From the drop-down list box, choose the calling search space for which you are adding a translation pattern, if necessary. If more 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 a calling search space name.</td>
</tr>
</tbody>
</table>

In Cisco Unified Communications Manager, you enable external call control by assigning an external call control profile to a translation pattern. If the translation pattern has an external call control profile assigned to it, when a call occurs that 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. For more information on external call control, see topics related to external call control in the *Cisco Unified Communications Manager Features and Services Guide*.

From the drop-down list box, choose the external call profile that you want to assign to the translation pattern.

**Route Option** The Route Option designation indicates whether you want this 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.

If you choose the **Block this pattern** radio button, you must choose the reason for which you want this translation pattern to block calls. Choose a value from the drop-down list box:

- No Error
- Unallocated Number
- Call Rejected
- Number Changed
- Invalid Number Format
- Precedence Level Exceeded

**Provide Outside Dial Tone** Outside dial tone indicates that Cisco Unified Communications Manager routes the calls off the local network. Check this check box for each translation pattern that you consider to be off network.
### Field | Description
--- | ---
Urgent Priority | 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.  
**Tip** 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.

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.

**Calling Party Transformations**

Use Calling Party's External Phone Number Mask | Check the check box if you want the full, external phone number to be used for calling line identification (CLID) on outgoing calls.

Calling Party Transform Mask | Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and 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.

Prefix Digits (Outgoing Calls) | Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +.  
**Note** The appended prefix digit does not affect which directory numbers route to the assigned device.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</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 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 topics related to calling party number transformations settings 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 topics related to device profile configuration settings and phone settings for information about the Ignore Presentation Indicators (internal calls only) field. For more information about call display restrictions, see topics related to call display restrictions in the *Cisco Unified Communications Manager System Guide*. |
| 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 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 calling party number transformations settings in the *Cisco Unified Communications Manager System Guide*. |
### 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 Unified Communications Manager**—The Cisco Unified Communications Manager sets the directory number type.
- **Unknown**—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.

### Calling Party Numbering Plan

Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—Use when the dialing plan is unknown.

### Connected Party Transformations
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Connected Line ID Presentation| 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 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.  
If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed.  
For more information about this field, see topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide*.  |
| Connected Name Presentation   | 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 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 topics related to connected party presentation and restriction settings in the *Cisco Unified Communications Manager System Guide*.  |
| Called Party Transformations   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Discard Digits                | Choose the discard digits instructions that you want to be associated with this translation pattern. See see topics related to discard digits instructions 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.  |
<p>| Called Party Transform Mask   | Enter a transformation mask value. Valid entries for the National Numbering Plan include the digits 0 through 9, and 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.  |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix Digits (Outgoing Calls)</td>
<td>Enter prefix digits. Valid entries for the National Numbering Plan include the digits 0 through 9, and the wildcard characters asterisk (*) and octothorpe (#); the international escape character +; and blank. <strong>Note</strong> The appended prefix digit does not affect which directory numbers route to the assigned device.</td>
</tr>
</tbody>
</table>
| Called Party Number Type                  | Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national type numbering plan. Choose one of the following options:  
  * Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type.  
  * Unknown—Use 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. |
| Called Party Numbering Plan               | Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options:  
  * Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.  
  * ISDN—Use when you are dialing outside the dialing plan for your country.  
  * National Standard—Use when you are dialing within the dialing plan for your country.  
  * Private—Use when you are dialing within a private network.  
  * Unknown—Use when the dialing plan is unknown. |
Related Topics

About route list setup, on page 183
Search for partition, on page 244
About calling search space setup, on page 247
Translation pattern setup, on page 251
Set up speed-dial buttons or abbreviated dialing, on page 582
About device profile setup, on page 663
Phone settings, on page 541
CHAPTER 44

Directory number setup

This chapter provides information about working with and configuring directory numbers (DNs) in Cisco Unified Communications Manager Administration.

For additional information, see topics related to directory numbers, Cisco Unified IP Phones, and phone features in the *Cisco Unified Communications Manager Administration System Guide*; as well as topics related to Cisco Unity connection configuration.

Additional information can also be found in *User Moves, Adds, and Changes Guide for Cisco Unity Connection* and topics related to presence in the *Cisco Unified Communications Manager Administration Features and Services Guide*.

- About directory number setup, page 263
- Directory number settings, page 265
- Synchronize directory number settings with devices, page 292
- Set up Private Line Automatic Ringdown (PLAR), page 293
- Remove directory number from phone, page 294
- Create Cisco Unity Connection voice mailbox, page 295

About directory number setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Directory Number** menu path to configure directory numbers (DNs).

Using Cisco Unified Communications Manager Administration, you configure and modify directory numbers (DNs) that are assigned to specific phones. Use the Directory Number Configuration window to perform the following tasks:

- Add or remove directory numbers.
- Assign directory URIs to a directory number
- Configure call forward, call pickup, call waiting, and multilevel precedence and preemption (MLPP) options.
- Set the display text that appears on the called party phone when a call is placed from a line.
• Configure ring settings.
• Configure Cisco Unity Connection voice mailboxes.

Shared lines always have identical DN settings, except for the field sections in the Directory Number Configuration window that contain the naming convention "on Device SEPXXXXXXXXXXXX," which are maintained/mapped to a specific device. If you add a shared line to a device, the shared DN configuration settings, such as Calling Search Space and Call Forward and Pickup, will display. If these DN configuration settings get changed, the new settings apply to all the shared lines.

**Assign directory URLs to a directory number**

Use the Directory Number Configuration window to associate directory URIs to a directory number. This allows Cisco Unified Communications Manager to support dialing using either the directory number or the directory URI. Each directory URI address must resolve to a single directory number in a partition.

**Directory number configuration tips**

You can configure the directory number configuration settings by choosing Call Routing > Directory Number; you can configure these settings after you add a phone under Call Routing > Phone; or, you can configure these settings after you add a CTI route point under Device > CTI Route Point.

If you configure the directory number via Device > Phone or Device > CTI Route Point, be aware that only the configuration settings that apply to your phone model or CTI route point display. If you configure the directory number via Call Routing > Directory Number, all of the directory number settings do not display at the same time; for example, after you configure the directory number and click Save, more configuration settings may display.

---

**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.

You can also add a directory number to a CTI route point by configuring the CTI route point under Device > CTI Route Point.

You can configure the call forward, call pickup, and MLPP phone features while you are adding the directory number.

**Tip**

You can assign patterns to directory numbers; for example, 352XX. To avoid user confusion when you assign a pattern to a directory number, add text or digits to the DN configuration fields, Line Text Label, Display (Internal Caller ID), and External Phone Number Mask. (These fields display for a directory number only after you add the directory number and you associate the 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.
If you need more than two lines, you can increase the lines by modifying the phone button template for the phone type (such as Cisco IP Phone 7960). Some phone types, however, only support one or two lines (such as Cisco IP Phone 7902).

Tip

Restart devices as soon as possible. During this process, the system may drop calls on gateways.

Note

Related Topics

- Synchronize directory number settings with devices, on page 292
- Set up Private Line Automatic Ringdown (PLAR), on page 293
- Remove directory number from phone, on page 294
- Create Cisco Unity Connection voice mailbox, on page 295
- Phone setup, on page 539

Directory number settings

The following table describes the fields that are available in the Directory Number Configuration window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number Information</td>
<td>Enter a dialable phone number. Values can include route pattern wildcards and numeric characters (0 through 9). Special characters such as a question mark (?), exclamation mark (!), backslash (), brackets ([ ]), plus sign (+), dash (-), asterisk (*), caret (^), pound sign (#), and an X are also allowable. Special characters that are not allowed are a period (.), at sign (@), dollar sign ($), and percent sign (%). At the beginning of the pattern, enter + if you want to use the international escape character +. For this field, + does not represent a wildcard; instead, entering + represents a dialable digit. Note When a pattern is used as a directory number, the display on the phone and the caller ID that displays on the dialed phone will both contain characters other than digits. To avoid this, Cisco recommends that you provide a value for Display (Internal Caller ID), Line text label, and External phone number mask. The directory number that you enter can appear in more than one partition. If you configure this field under Call Routing &gt; Directory Number, you can enter insert directory numbers in bulk by entering a range (that is, by entering the beginning directory number in the first field and by entering the ending directory number in the second field); by using this method, you can create up to 500 directory numbers at a time.</td>
</tr>
</tbody>
</table>
### Directory number settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Partition</td>
<td>Choose the partition to which the directory number belongs. Make sure that the directory number that you enter in the Directory Number field is unique within the partition that you choose. If you do not want to restrict access to the directory number, choose &lt;None&gt; 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, then find and choose a partition name. <strong>Note</strong> To set the maximum list box items, choose <strong>System &gt; Enterprise Parameters</strong> and choose CCMAdmin Parameters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the directory number and 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>
<tr>
<td>Alerting Name</td>
<td>Enter a name that you want to display on the phone of the caller when the called phone is ringing. This setting, which supports the Identification Services for the QSIG protocol, applies to shared and nonshared directory numbers. When the phone rings at the terminating PINX, if you configured an alerting name for a directory number with shared-line appearances, the system performs the following tasks: • Forwards the alerting name of the called party, if configured, to the caller. • Applies the Connected Name Restrictions (CONR) that are configured for the translation pattern (if restrictions exist) Depending on the state of the call and your configuration, the alerting name, directory number, or display (internal caller ID) configuration may display on the phone, as described in the following bullets. • Alerting state—The alerting name displays, as configured in the Directory Number window. • Connected state—If you configure the Display (Internal Caller ID) and the Alerting Name fields, the display (internal caller ID) name displays. • Connected State—If you configured the Alerting Name field but not the Display (Internal Caller ID) field, the directory number displays. If you set the Always Display Original Dialed Number service parameter to True, the original dialed number and the alerting name displays during the call. You can choose if the alerting name for the original dialed number or the translated dialed number is displayed using the Cisco CallManager service parameter called Name Display for Original Dialed Number When Translated. The default setting displays the alerting name of the original dialed number before translation. <strong>Note</strong> Do not use the word &quot;Voicemail&quot; anywhere in your Alerting Name or ASCII Alerting Name. Use of the word &quot;Voicemail&quot; can cause Cisco Unity Connection to process the call as a direct call rather than as a forwarded call.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.  

**Note** Do not use the word "Voicemail" anywhere in your Alerting Name or ASCII Alerting Name. Use of the word "Voicemail" can cause Cisco Unity Connection to process the call as a direct call rather than as a forwarded call. |
| Active                        | To view this check box on the Directory Number Configuration window, access an unassigned directory number from the Route Plan Report window. Checking this check box allows calls to this DN to be forwarded (if forwarding is configured). If check box is not checked, Cisco Unified Communications Manager ignores the DN. |
| 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 directory number is associated  

If the directory number specifies a shared line, ensure the check box is enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports. |
| Line Group                    | From this drop-down list box, choose a line group with which to associate this DN.  

To edit or view the line group information for a line group, choose a line group from the drop-down list box and click the Edit Line Group button.  

**Note** If you configure a DN as part of a line group, you will not be able to associate that DN with a CTI port nor a CTI route point. Conversely, when you configure a CTI port or CTI route point, you will not be able to specify a DN that already belongs to a line group or to a hunt list. Furthermore, if a DN is a member of a line group or hunt list, any device (CTI port, CTI route point, phone that is running SCCP, or phone that is running SIP) that uses that DN should not be associated with a CTI user. |
| Associated Devices            | After you associate this DN with a device(s), this pane displays the devices with which this DN is associated.  

To edit a device with which this DN 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.  

To edit a line appearance that has been defined for this DN, 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 DN 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. |
### Directory number settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissociate Devices</td>
<td>If you choose to dissociate a DN from a device, this pane displays the device(s) from which you dissociate this DN. 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.</td>
</tr>
</tbody>
</table>

#### Directory Number Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Mail Profile</td>
<td>Choose from list of Voice Mail Profiles that the Voice Mail Profile Configuration defines. The first option specifies &lt;None&gt;, which represents the current default Voice Mail Profile that is configured in the Voice Mail Profile Configuration.</td>
</tr>
</tbody>
</table>
| Calling Search Space| From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number. 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 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 topics related to partitions and calling search spaces in the *Cisco Unified Communications Manager System Guide*.
<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 directory number. The selected group specifies the devices, end users, and application users that can monitor this 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 topics related to presence in the Cisco Unified Communications Manager System Guide for information about configuring permissions between groups.</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
<td>Choose the audio source that plays when a user initiates a hold action.</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
<td>Choose the audio source that plays when the network initiates a hold action.</td>
</tr>
<tr>
<td>Auto Answer</td>
<td>Choose one of the following options to activate the Auto Answer feature for this directory number:</td>
</tr>
<tr>
<td></td>
<td>• Auto Answer Off &lt;Default&gt;</td>
</tr>
<tr>
<td></td>
<td>• Auto Answer with Headset</td>
</tr>
<tr>
<td></td>
<td>• Auto Answer with Speakerphone</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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><strong>Note</strong></td>
<td>Do not configure Auto Answer for devices that have shared lines.</td>
</tr>
<tr>
<td>Directory URIs</td>
<td></td>
</tr>
</tbody>
</table>
### Directory URIs

The fields in this section can be completed to associate directory URIs to a directory number so that users can make calls and identify callers using directory URIs rather than directory numbers. Users can associate up to five separate directory URIs to a single directory number, but they must select a primary URI.

To associate a directory URI to the directory number, enter the directory URI in the URI text box, select the partition on which the URI is saved, and click **Save**.

The Directory URIs section contains the following fields and buttons:

- **Primary**—Check this radio button to select the primary directory URI for instances where more than one directory URI is associated to a directory number.
- **URI**—Enter the directory URI address in this text box. For detailed information on valid directory URI formats, see Directory URI format.
- **Partition**—From the drop-down menu, choose the partition to which the directory URI belongs. Make sure that the directory URI that you enter is unique within the partition that you choose. If you do not want to restrict access to the URI, choose **<None>** for the partition.
- **Remove**—Click the (−) button to delete this directory URI from the directory number configuration. After the directory URI has been deleted, click **Save**.
- **Add Row**—When you want to associate multiple directory URIs to the directory number, click this button to add new rows on which you can enter the additional directory URIs.

For detailed information on valid formats for directory URIs, see the "Directory URI Format" topic in the Intercluster Directory URI chapter of the Cisco Unified Communications Manager Administration Guide.

### AAR Settings

The settings in this row of fields specify treatment of calls for which insufficient bandwidth exists to reach the destination. Automated alternate routing (AAR) handles these calls that are routed to the AAR Destination Mask or Voice Mail.

Configure the following values:

- **Voice Mail**—Check this check box to use settings in the Voice Mail Profile Configuration window. When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Coverage/Destination box and Calling Search Space.
- **AAR Destination Mask**—Use this setting instead of the external phone number mask to determine the AAR Destination to be dialed.
- **AAR Group**—This setting provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None indicates that no rerouting of blocked calls will be attempted.
This setting determines whether the AAR leg of the call will be present in the call forwarding history. If you uncheck the check box, the AAR leg of the call is not present in the call history. If you check the check box, the AAR leg of the call will be present in the call history.

By default, the directory number configuration retains the AAR leg of the call in the call history, which ensures that the AAR forward to voice-messaging system will prompt the user to leave a voice message.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retain this destination in the call forwarding history</td>
<td>This setting determines whether the AAR leg of the call will be present in the call forwarding history. If you uncheck the check box, the AAR leg of the call is not present in the call history. If you check the check box, the AAR leg of the call will be present in the call history. By default, the directory number configuration retains the AAR leg of the call in the call history, which ensures that the AAR forward to voice-messaging system will prompt the user to leave a voice message.</td>
</tr>
</tbody>
</table>

Call Forward and Call Pickup Settings
## Directory number settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Search Space</td>
<td></td>
</tr>
<tr>
<td>Activation Policy</td>
<td></td>
</tr>
</tbody>
</table>
Three possible values exist for this option:

- Use System Default
- With Configured CSS
- With Activating Device/Line CSS

If you select the With Configured CSS option, the Forward All Calling Search Space that is explicitly configured in the Directory Number Configuration window controls the forward all activation and call forwarding. If the Forward All Calling Search Space is set to None, no CSS gets configured for Forward All. A forward all activation attempt to any directory number with a partition will fail. No change in the Forward All Calling Search Space and Secondary Calling Search Space for Forward All occurs during the forward all activation.

If you prefer to utilize the combination of the Directory Number Calling Search Space and Device Calling Search Space without explicitly configuring a Forward All Calling Search Space, select With Activating Device/Line CSS for the Calling Search Space Activation Policy. With this option, when Forward All is activated from the phone, the Forward All Calling Search Space and Secondary Calling Search Space for Forward All automatically gets populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device.

With this configuration (Calling Search Space Activation Policy set to With Activating Device/Line), if the Forward All Calling Search Space is set to None, when forward all is activated through the phone, the combination of Directory Number Calling Search Space and activating Device Calling Search Space gets used to verify the forward all attempt.

If you configure the Calling Search Space Activation Policy to Use System Default, then the CFA CSS Activation Policy cluster-wide service parameter determines which Forward All Calling Search space will be used. If the CFA CSS Activation Policy service parameter gets set to With Configured CSS, then Forward All Calling Search Space and Secondary Calling Search Space for Forward All will be used for Call Forwarding. If CFA CSS Activation Policy service parameter gets set to With Activating Device/Line CSS, then Forward All Calling Search Space and Secondary Calling Search Space for Forward All will be automatically populated with the Directory Number Calling Search Space and Device Calling Search Space for the activating device.

CFA CSS Activation Policy Service Parameter:

Ensure the CFA CSS Activation Policy service parameter that displays in the Clusterwide Parameters (Feature - Forward) section of the Service Parameter Configuration window is set correctly for call forward all to work as intended. The parameter includes two possible values:

- With Configured CSS (default)
- With Activating Device/Line CSS

When the Calling Search Space Activation Policy is set to Use System Default, the value of the CFA CSS Activation Policy service parameter gets used to determine
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>the Call Forward All CSS.</td>
</tr>
<tr>
<td></td>
<td>When the option With Configured CSS is selected, the primary and secondary CFA Calling Search Space get used. When the option With Activating Device/Line CSS is selected, the primary and secondary CFA Calling Search Space get updated with primary line Calling Search Space and activating Device Calling Search Space.</td>
</tr>
<tr>
<td></td>
<td>By default, the value of the CFA CSS Activation Policy service parameter is set to With Configured CSS.</td>
</tr>
<tr>
<td></td>
<td><strong>Roaming:</strong></td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• The Device CSS and Line CSS get used as the CFA CSS when the device is in its home location.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• If the device is roaming within a different device mobility group, the Device CSS and Line CSS get used as the CFA CSS.</td>
</tr>
<tr>
<td></td>
<td><strong>Forward All</strong></td>
</tr>
<tr>
<td></td>
<td>The settings in this row of fields specify the forwarding treatment for calls to this directory number if the directory number is set to forward all calls. The Calling Search Space field gets used to validate the Forward All destination that is entered when the user activates Call Forward All from the phone. This field also gets used to redirect the call to the Call Forward All destination.</td>
</tr>
<tr>
<td></td>
<td>Specify the following values:</td>
</tr>
<tr>
<td></td>
<td>• Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space.</td>
</tr>
<tr>
<td></td>
<td>• Destination—This setting indicates the directory number to which all calls are forwarded. Use any dialable phone number, including an outside destination.</td>
</tr>
<tr>
<td></td>
<td>• Calling Search Space—This setting applies to all devices that are using this directory number.</td>
</tr>
</tbody>
</table>
Because call forwarding is a line-based feature, in cases where the device calling search space is unknown, the system uses only the line calling search space to forward the call. If the line calling search space is restrictive and not routable, the forward attempt fails.

Addition of a secondary calling search space for Call Forward All provides a solution to enable forwarding. The primary calling search space for Call Forward All and secondary calling search space for Call Forward All get concatenated (Primary CFA CSS + Secondary CFA CSS). Cisco Unified Communications Manager uses this combination to validate the CFA destination and to forward the call.

See the description for the Calling Search Space field for information about how the combination of Primary and Secondary CFA CSSs works.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Calling Search Space for Forward All</td>
<td>Because call forwarding is a line-based feature, in cases where the device calling search space is unknown, the system uses only the line calling search space to forward the call. If the line calling search space is restrictive and not routable, the forward attempt fails. Addition of a secondary calling search space for Call Forward All provides a solution to enable forwarding. The primary calling search space for Call Forward All and secondary calling search space for Call Forward All get concatenated (Primary CFA CSS + Secondary CFA CSS). Cisco Unified Communications Manager uses this combination to validate the CFA destination and to forward the call. See the description for the Calling Search Space field for information about how the combination of Primary and Secondary CFA CSSs works.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Forward Busy Internal | The settings in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number is busy. See the description for the Busy Trigger field for information on when a line is considered busy. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values:  
  • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window for internal calls.  
  Note When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space.  
  Note When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls.  
  • Destination—This setting indicates the call forward busy destination for internal calls. Use any dialable phone number, including an outside destination.  
  Note When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls.  
  • Calling Search Space—The Forward Busy internal Calling Search Space is used to forward the call to the Forward Busy Internal destination. It applies to all devices that are using this directory number.  
  Note If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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.  
  Note When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box. |
### Directory number settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forward Busy External</strong></td>
<td>The settings in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number is busy. See the description for the Busy Trigger field for information on when a line is considered busy. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values:</td>
</tr>
<tr>
<td><strong>Voice Mail</strong></td>
<td>• Check this check box to use settings in the Voice Mail Profile Configuration window for external calls.</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td>• This setting indicates the call forward busy destination for external calls. Use any dialable phone number, including an outside destination.</td>
</tr>
<tr>
<td><strong>Calling Search Space</strong></td>
<td>• The Forward Busy external Calling Search Space is used to forward the call to the Forward Busy External destination. It applies to all devices that are using this directory number.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When the Voice Mail check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Forward No Answer</td>
<td>The settings in this row of fields specify the forwarding treatment for internal calls to this directory number if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values:</td>
</tr>
<tr>
<td>Internal</td>
<td>- Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window.</td>
</tr>
<tr>
<td>Note</td>
<td>When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space.</td>
</tr>
<tr>
<td>Note</td>
<td>When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls.</td>
</tr>
<tr>
<td>Note</td>
<td>When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls.</td>
</tr>
<tr>
<td>Note</td>
<td>- Destination—This setting indicates the directory number to which an internal call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination.</td>
</tr>
<tr>
<td>Note</td>
<td>- Calling Search Space—The Forward No Answer internal Calling Search Space is used to forward the call to the Forward No Answer internal destination. It applies to all devices that are using this directory number.</td>
</tr>
<tr>
<td>Note</td>
<td>If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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 No Answer destination, you should also configure the Forward No Answer Calling Search Space. If you do not configure the Forward No Answer Calling Search Space, and the Forward No Answer destination is in a partition, the forward operation may fail.</td>
</tr>
<tr>
<td>Note</td>
<td>When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box for external calls.</td>
</tr>
</tbody>
</table>
### Directory number settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward No Answer External</td>
<td>The settings in this row of fields specify the forwarding treatment for external calls to this directory number if the directory number does not answer. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values:</td>
</tr>
</tbody>
</table>

- **Voice Mail**—Check this check box to use settings in the Voice Mail Profile Configuration window. |

**Note** When this check box is checked, the calling search space of the voice mail pilot gets used. Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. |

**Note** When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls. |

- **Destination**—This setting indicates the directory number to which an external call is forwarded when the call is not answered. Use any dialable phone number, including an outside destination. |

**Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls. |

- **Calling Search Space**—The Forward No Answer external Calling Search Space is used to forward the call to the Forward No Answer external destination. It applies to all devices that are using this directory number. |

**Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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 No Answer destination, you should also configure the Forward No Answer Calling Search Space. If you do not configure the Forward No Answer Calling Search Space, and the Forward No Answer destination is in a partition, the forward operation may fail. |

**Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, you must choose a different setting in the Calling Search Space drop-down list box for external calls.
### Directory number settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Forward No Coverage Internal | For complete information about Call Coverage, the *Cisco Unified Communications Manager System Guide*. The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values:  
  • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window.  
  
  **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls.  
  
  • Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination.  
  
  **Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls.  
  
  • Calling Search Space—The Forward No Coverage internal Calling Search Space is used to forward the call to the Forward No Coverage internal destination. This setting applies to all devices that are using this directory number.  
  
  **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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 No Coverage destination, you should also configure the Forward No Coverage Calling Search Space. If you do not configure the Forward No Coverage Calling Search Space, and the Forward No Coverage destination is in a partition, the forward operation may fail.  
  
  **Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, choose a different setting in the Calling Search Space for external calls. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Forward No Coverage External | For complete information about Call Coverage, the Cisco Unified Communications Manager System Guide.  
The call forward destination and Calling Search Space field get used to redirect the call to the forward destination. Specify the following values:  
  • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window.  
  
  **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space. When this check box is checked for internal calls, the system automatically checks the Voice Mail check box for external calls. If you do not want external calls to forward to the voice-messaging system, you must uncheck the Voice Mail check box for external calls.  
  
  • Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination.  
  
  **Note** When you enter a destination value for internal calls, the system automatically copies this value to the Destination field for external calls. If you want external calls to forward to a different destination, you must enter a different value in the Destination field for external calls.  
  
  • Calling Search Space—The Forward No Coverage external Calling Search Space is used to forward the call to the Forward No Coverage external destination. This setting applies to all devices that are using this directory number.  
  
  **Note** If the system is using partitions and calling search spaces, Cisco recommends that you configure the forward calling search spaces. 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 No Coverage destination, you should also configure the Forward No Coverage Calling Search Space. If you do not configure the Forward No Coverage Calling Search Space, and the Forward No Coverage destination is in a partition, the forward operation may fail.  
  
  **Note** When you choose a Calling Search Space for internal calls, the system automatically copies this setting to the Calling Search Space setting for external calls. If you want external calls to forward to a different calling search space, choose a different setting in the Calling Search Space for external calls. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Forward on CTI Failure            | This field applies only to CTI route points and CTI ports. The settings in this row specify the forwarding treatment for external calls to this CTI route point or CTI port if the CTI route point or CTI port fails. Specify the following values:  
  • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window.  
  **Note** When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space.  
  • Destination—This setting specifies the directory number to which an internal nonconnected call is forwarded when an application that controls that directory number fails. Use any dialable phone number, including an outside destination.  
  • Calling Search Space—This setting applies to all devices that are using this directory number.                                                                                                                                                                                   |
| Forward Unregistered Internal     | This field applies to unregistered internal DN calls. The calls are rerouted to a specified Destination Number or Voice Mail.  
  **Note** You must also specify the maximum number of forwards in the Service Parameters Configuration window for a Directory Number.                                                                                                                                                                                   |
| Forward Unregistered External     | This field applies to unregistered external DN calls. The calls are rerouted to a specified Destination Number or Voice Mail.  
  **Note** You must also specify the maximum number of forwards in the Service Parameters Configuration window for a Directory Number.                                                                                                                                                                                   |
| No Answer Ring Duration (seconds) | Used in conjunction with Call Forward No Answer Destination, this field sets the timer for how long the phone will ring before it gets forwarded. Leave this setting blank to use the value that is set in the Cisco CallManager service parameter, Forward No Answer Timer.  
  **Caution** By default, Cisco Unified Communications Manager makes the time for the T301 timer longer than the No Answer Ring Duration time; if the set time for the T301 timer expires before the set time for the No Answer Ring Duration expires, the call ends, and no call forwarding can occur. If you choose to do so, you can configure the time for the No Answer Ring Duration to be greater than the time for the T301 timer. For information on the T301 timer, choose System > Service Parameters; choose the server, the Cisco CallManager service, and then the parameter in the window that displays. |
<p>| Call Pickup Group                 | Choose the number that can be dialed to answer calls to this directory number (in the specified partition).                                                                                                                                                                                                                           |
| Park Monitoring                   |                                                                                                                                                                                                                                                                                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Park Monitoring Forward No Retrieve Destination External | When the parkee is an external party, the call will be forwarded to the specified destination in this field. If this field value is empty, the parkee will be redirected to the Parker’s line. Specify the following values:  
  • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window.  
**Note**  
  When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space.  
  • Destination—This setting specifies the directory number to which a parked call (from an external party) is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination.  
  • Calling Search Space—A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. |
| Park Monitoring Forward No Retrieve Destination Internal | When the parkee is an internal party, the call will be forwarded to the specified destination in this field. If this field value is empty, the parkee will be redirected to the Parker’s line. Specify the following values:  
  • Voice Mail—Check this check box to use settings in the Voice Mail Profile Configuration window.  
**Note**  
  When this check box is checked, Cisco Unified Communications Manager ignores the settings in the Destination box and Calling Search Space.  
  • Destination—This setting specifies the directory number to which a parked call (from an internal party) is forwarded when the service parameter Park Monitoring Forward No Retrieve Timer expires. Use any dialable phone number, including an outside destination.  
  • Calling Search Space—A calling search space comprises an ordered list of route partitions that are typically assigned to devices. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. |
### Directory number settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Park Monitoring Reversion Timer | 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.  
  The default is 60 seconds.  
  **Note** If you configure a non-zero value, this value overrides the value of this parameter set in the Service Parameters window. However, if you configure a value of 0 here, then the value in the Service Parameters window will be used. |
| MLPP Alternate Party Settings  |                                                                                                                                                                                                          |
| Target (Destination)          | Enter the number to which MLPP precedence calls should be diverted if this directory number receives a precedence call and neither this number nor its call forward destination answers the precedence call.  
  Values can include numeric characters, octothorpe (#), and asterisk (*). |
| MLPP Calling Search Space     | From the drop-down list box, choose the calling search space to associate with the MLPP alternate party target (destination) number.                                                                   |
| MLPP No Answer Ring Duration (seconds) | Enter the number of seconds (between 4 and 60) after which an MLPP precedence call will be directed to this directory number alternate party if this directory number and its call-forwarding destination have not answered the precedence call.  
  Leave this setting blank to use the value that is set in the Cisco Unified Communications Manager enterprise parameter, Precedence Alternate Party Timeout. |
| Line Settings for All Devices |                                                                                                                                                                                                          |
| Hold Reversion Ring Duration (seconds) | Enter a number from 0 to 1200 (inclusive) to specify the wait time in seconds before issuing a reverted call alert to the holding party phone.  
  If you enter a value of 0, Cisco Unified Communications Manager does not invoke the reverted call feature for a held call.  
  At installation, this field remains blank. If you leave this setting blank, the Hold Reversion Duration timer setting for the cluster applies. |
| Hold Reversion Notification Interval (seconds) | Enter a number from 0 to 1200 (inclusive) to specify the interval time in seconds for sending periodic reminder alerts to the holding party phone.  
  If you enter a value of 0, Cisco Unified Communications Manager does not send reminder alerts.  
  At installation, this field remains blank. If you leave this setting blank, the Hold Reversion Notification Interval timer setting for the cluster applies.  
  **Note** SCCP phones support a minimum Hold Reversion Notification Interval (HRNI) of 5 seconds, whereas SIP phones support a minimum of 10 seconds.  
  SCCP phones set for the minimum HRNI of 5 seconds may experience a Hold Reversion Notification ring delay of 10 seconds when handling calls involving SIP phones. |

---

SCCP phones support a minimum Hold Reversion Notification Interval (HRNI) of 5 seconds, whereas SIP phones support a minimum of 10 seconds. SCCP phones set for the minimum HRNI of 5 seconds may experience a Hold Reversion Notification ring delay of 10 seconds when handling calls involving SIP phones.
### Party Entrance Tone

From the Party Entrance Tone drop-down list box, choose one of the following options:

- **Default**—Use the value that you configured in the Party Entrance Tone service parameter.
- **On**—A tone plays on the phone when a basic call changes to a multi-party call; that is, a barge call, eBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multi-party call. If the controlling device, that is, the originator of the multi-party call has a built-in bridge, the tone gets played to all parties if you choose On 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.
- **Off**—A tone does not play on the phone when a basic call changes to a multi-party call.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Party Entrance Tone</td>
<td>From the Party Entrance Tone drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Default—Use the value that you configured in the Party Entrance Tone service parameter.</td>
</tr>
<tr>
<td></td>
<td>• On—A tone plays on the phone when a basic call changes to a multi-party call; that is, a barge call, eBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multi-party call. If the controlling device, that is, the originator of the multi-party call has a built-in bridge, the tone gets played to all parties if you choose On 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.</td>
</tr>
<tr>
<td></td>
<td>• Off—A tone does not play on the phone when a basic call changes to a multi-party call.</td>
</tr>
</tbody>
</table>

### Line [number] on Device [device name]

**Note** These fields display only after you associate this directory number with a device.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display (Internal Caller ID)</td>
<td>Leave this field blank to have the system display the extension. Use a maximum of 30 characters. Typically, use the user name or the directory number (if using the directory number, the person receiving the call may not see the proper identity of the caller). Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII Display (Internal Caller ID)</td>
<td>This field provides the same information as the Display (Internal Caller ID) field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the ASCII Display (Internal Caller ID) field. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Line Text Label</td>
<td>Use this field only if you do not want the directory number to show on the line appearance. Enter text that identifies this directory number for a line/phone combination. Suggested entries include boss name, department name, or other appropriate information to identify multiple directory numbers to secretary/assistant who monitors multiple directory numbers. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)</td>
</tr>
<tr>
<td>ASCII Line Text Label</td>
<td>This field provides the same information as the Line Text Label field, but you must limit input to ASCII characters. Devices that do not support Unicode (internationalized) characters display the content of the ASCII Line Text Label field. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)</td>
</tr>
<tr>
<td>External Phone Number Mask</td>
<td>Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 number, the international escape character +, and “X” characters. The Xs represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234. Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)</td>
</tr>
</tbody>
</table>
| Visual Message Waiting Indicator Policy | Use this field to configure the handset lamp illumination policy. Choose one of the following options:  
- Use System Policy (The directory number refers to the service parameter "Message Waiting Lamp Policy" setting.)  
- Light and Prompt  
- Prompt Only  
- Light Only  
- None  
Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.) |
### Directory number settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audible Message Waiting Indicator Policy</td>
<td>Use this field to configure an audible message waiting indicator policy. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Off</td>
</tr>
<tr>
<td></td>
<td>• On—When you select this option, you will receive a stutter dial tone when you take the handset off hook.</td>
</tr>
<tr>
<td></td>
<td>• Default—When you select this option, the phone uses the default that was set at the system level.</td>
</tr>
<tr>
<td>Ring Setting (Phone Idle)</td>
<td>Use this field to configure the ring setting for the line appearance when an incoming call is received and no other active calls exist on that device. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Use system default</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td></td>
<td>• Flash only</td>
</tr>
<tr>
<td></td>
<td>• Ring once</td>
</tr>
<tr>
<td></td>
<td>• Ring</td>
</tr>
<tr>
<td></td>
<td>Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)</td>
</tr>
<tr>
<td>Note</td>
<td>Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.</td>
</tr>
<tr>
<td>Ring Setting (Phone Active)</td>
<td>From the drop-down list box, choose the ring setting that is used when this phone has another active call on a different line. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Use system default</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td></td>
<td>• Flash only</td>
</tr>
<tr>
<td></td>
<td>• Ring once</td>
</tr>
<tr>
<td></td>
<td>• Ring</td>
</tr>
<tr>
<td></td>
<td>• Beep only</td>
</tr>
<tr>
<td></td>
<td>Setting applies only to the current device unless you check the check box at right (Update Shared Device Settings) and click the Propagate Selected button. (The check box at right displays only if other devices share this directory number.)</td>
</tr>
<tr>
<td>Note</td>
<td>Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call Pickup Group Audio Alert Setting (Phone Idle)</td>
<td>This field determines the type of notification an incoming call sends to members of a call pickup group. If the called phone does not answer, the phones in the call pickup group that are idle will either hear a short ring (ring once) or hear nothing (disabled).</td>
</tr>
<tr>
<td></td>
<td>• Use System Default—The value of this field gets determined by the setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Idle Station.</td>
</tr>
<tr>
<td></td>
<td>• Disable—No alert is sent to members of the call pickup group.</td>
</tr>
<tr>
<td></td>
<td>• Ring Once—A short ring is sent to members of the call pickup group.</td>
</tr>
<tr>
<td>Call Pickup Group Audio Alert Setting (Phone Active)</td>
<td>This field determines the type of notification an incoming call sends to members of a call pickup group. If the called phone does not answer, the phones in the call pickup group that are busy will either hear a beep (beep beep) or hear nothing (disabled).</td>
</tr>
<tr>
<td></td>
<td>• Use System Default—The value of this field gets determined by the setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Busy Station.</td>
</tr>
<tr>
<td></td>
<td>• Disable—No alert is sent to member of the call pickup group.</td>
</tr>
<tr>
<td></td>
<td>• Beep Only—A beep beep is sent to members of the call pickup group.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Recording Option | This field determines the recording option on the line appearance of an agent. The default recording option is Call Recording Disabled. Choose one of the following options:
- Call Recording Disabled—Calls made on this line appearance cannot be recorded.
- Automatic Call Recording Enabled—Calls made on this line appearance are recorded automatically.
- Selective Call Recording Enabled—Calls made on this line appearance can be recorded using a softkey or programmable line key that is assigned to the device, a CTI-enabled application, or both interchangeably.

Selective recording supports two modes:
- Silent recording—Call recording status is not reflected on the Cisco IP device display. Silent recording is typically used in a call center environment to allow a supervisor to record an agent call. A CTI-enabled application running on the supervisor desktop is generally used to start and stop the recording for an agent-customer call.
- User recording—Call recording status is reflected on the Cisco IP device display. A recording can be started or stopped using a softkey, programmable line key, or CTI-enabled application running on the user desktop. To enable user recording, add the Record softkey or programmable line key to the device template. Do not add the Record key if only silent recording is desired.

When the recording option is set to either Automatic Call Recording Enabled or Selective Call Recording Enabled, the line appearance can be associated with a recording profile.

When automatic recording is enabled, start- and stop-recording requests using a softkey, programmable line key, or CTI-enabled application are rejected.

Recording Profile | This field determines the recording profile on the line appearance of an agent. Choose an existing recording profile from the drop-down list box. To create a recording profile, use the Device > Device Settings > Recording Profile menu option.

The default value specifies None.

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. Choose an existing calling search space from the drop-down list box.

The default value specifies None.

Log Missed Calls | If the check box displays as checked, which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for the shared line appearance on the phone. If you uncheck the check box, missed calls do not get logged to the shared line appearance.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Call/Call Waiting Settings on Device [device name]</td>
<td>Note: These fields display only after you associate this directory number with a device.</td>
</tr>
<tr>
<td>Maximum Number of Calls</td>
<td>You can configure up to 200 calls for a line on a device, with the limiting factor being the total number of calls that are configured on the device. As you configure the number of calls for one line, the calls that are available for another line decrease. The default specifies 4. If the phone does not allow multiple calls for each line, the default specifies 2. For CTI route points, you can configure up to 10,000 calls for each port. The default specifies 5000 calls. Use this field in conjunction with the Busy Trigger field. Note: Although the default specifies 5000 calls for maximum number of active calls that can be configured on a CTI route point, Cisco recommends that you set the maximum number of calls to no more than 200 per route point. This will prevent system performance degradation. If the CTI application needs more than 200 calls, Cisco recommends that you configure multiple CTI route points. Tip: If you use the external call control feature, and the policies on the policy server dictate that a chaperone must monitor and record calls, make sure that you set the Maximum Number of Calls setting to 2 and set the Busy Trigger setting to 1.</td>
</tr>
<tr>
<td>Busy Trigger</td>
<td>This setting, which works in conjunction with Maximum Number of Calls and Call Forward Busy, determines the maximum number of calls to be presented at the line. If maximum number of calls is set for 50 and the busy trigger is set to 40, incoming call 41 gets rejected with a busy cause (and will get forwarded if Call Forward Busy is set). If this line is shared, all the lines must be busy before incoming calls get rejected. Use this field in conjunction with Maximum Number of Calls for CTI route points. The default specifies 4500 calls. Tip: To review how this setting works for devices with shared line appearances, see topics related to shared line appearance in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Forwarded Call Information Display on Device [device name]</td>
<td>Note: These fields display only after you associate this directory number with a device.</td>
</tr>
<tr>
<td>Caller Name</td>
<td>Checking this check box will cause the caller name to display upon call forward.</td>
</tr>
<tr>
<td>Caller Number</td>
<td>Checking this check box will cause the caller number to display upon call forward.</td>
</tr>
<tr>
<td>Redirected Number</td>
<td>Checking this check box will cause the number that was redirected to display upon call forward.</td>
</tr>
<tr>
<td>Dialed Number</td>
<td>Checking this check box will cause the original dialed number to display upon call forward.</td>
</tr>
</tbody>
</table>
### Field Description

**Users Associated with Line**

This information displays only after you associate this directory number with a device.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| (user name)            | This pane displays the end users that are associated with this line. To associate end users with this line, click the Associate End Users button, which causes the Find and List Users popup window to display. In the popup window, you can use the Find function to find end users to associate with this line. After you have found the end users to associate with this line, click the Add Selected button, and the selected end users will be added to the Users Associated with Line pane for this line. For each associated end user, the following information displays:

- **Full Name**—This column displays the last name and first name entries for the associated end user.
- **User ID**—This column displays the user ID of the associated end user.
- **Permission**—Click the i button to display the user privilege information for this end user.

After at least one end user has been associated with this line, the following additional buttons display:

- **Select All**—Click this button to select all end users that are associated with this line.
- **Clear All**—Click this button to deselect all end users that are associated with this line.
- **Delete Selected**—After selecting any end users that you wish to dissociate from this line, click this button. Doing so dissociates the end users from this line, but does not delete the end user records. |

### Related Topics

- Service parameter setup, on page 131
- Line group setup, on page 201
- Search for partition, on page 244
- Display calling search space, on page 291
- Cisco Unified IP Phone setup, on page 537
- Device profile setup, on page 663
- About end user setup, on page 771
- Directory URI format, on page 323

### Display calling search space

You can configure the number of calling search spaces 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...
Synchronize directory number settings with devices

To synchronize devices with a directory number that has undergone configuration changes, perform the following procedure, which applies 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 > Directory Number Configuration.  
The Find and List Directory Numbers window displays.

Step 2  Choose the search criteria to use.

Step 3  Click Find.  
The window displays a list of directory numbers that match the search criteria.

Step 4  Click the directory number to which you want to synchronize applicable devices. The 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.  

   Note  If devices require a restart, the system may drop active calls on gateways.

Step 8  Click OK.

Related Topics

Directory number setup, on page 263
Set up Private Line Automatic Ringdown (PLAR)

You can configure Private Line Automatic Ringdown (PLAR), so 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 the phone line that gets configured for PLAR.

PLAR works with features such as barge, cBarge, or single button barge. If you use PLAR with a feature, you must configure the feature as described in the feature documentation, and you must configure the PLAR destination, which is a directory number that is used specifically for PLAR.

See the example of how to configure PLAR, which describes how to enable PLAR functionality for phones that support barge and that are running SCCP and SIP.

Related Topics
- Set up PLAR example, on page 293

Set up PLAR example

This example of how to configure PLAR describes how to enable PLAR functionality for phones that support barge and that are running SCCP and SIP. A and A’ represent shared-line devices that you configured for barge, and B1 represents the directory number for the PLAR destination. Follow this example to enable PLAR functionality from A/A’.

Tip

Set up PLAR example, on page 293 through Set up PLAR example, on page 293 apply if you want to configure PLAR for phones that are running SCCP. For phones that are running SIP, you must perform Set up PLAR example, on page 293 through Set up PLAR example, on page 293. Before you attempt to configure PLAR, verify that your phone model supports PLAR. To determine whether your phone supports PLAR, see the Cisco Unified IP Phone Administration Guide that supports your phone model and this release of Cisco Unified Communications Manager.

Procedure

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 null (blank) translation pattern, for example, TP1, which contains calling search space CSS1 and partition P1. In this null (blank) pattern, make sure that you enter the directory number for the B1 PLAR
Step 3 Assign the called party search space, CS1, to either A or A’. (In Cisco Unified Communications Manager Administration, choose Call Routing > Translation Pattern.)

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.)

Related Topics
Directory number setup, on page 263

Remove directory number from phone

Perform the following procedure to remove a directory number (DN) from a specific phone.

Before You Begin
If you try to remove a directory number that is in use, Cisco Unified Communications Manager displays a message. To find out which line groups are using the directory number, click the Dependency Records link from the Directory Number Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

When you remove a directory number from a phone, the number still exists within Cisco Unified Communications Manager. To see a list of directory numbers that are not associated with phones, use the Route Plan Report menu option.

Procedure

Step 1 Choose Device > Phone. The Find and List Phones window displays.

Step 2 To locate a specific phone, enter the search criteria and click Find. A list of phones that match the search criteria displays.

Step 3 Choose the device name that contains the directory number that you want to remove. The Phone Configuration window displays.

Step 4 In the Association Information area on the left, choose the line that you want to remove. The Directory Number Configuration window displays.

Step 5 In the Associated Devices pane, choose the device name of the phone from which you want to remove this directory number.

Step 6 Click the down arrow below the Associated Devices pane.
The phone name moves to the Dissociate Devices pane.

**Step 7**

Click the Save button at the bottom of the Directory Number Configuration window.

The Phone Configuration window displays with the directory number removed. The change gets automatically applied to the phone; however, you can click Reset Phone.

---

**Related Topics**

- Directory number setup, on page 263
- Delete unassigned directory number, on page 307
- Phone setup, on page 539
- Access dependency records, on page 874

---

**Create Cisco Unity Connection voice mailbox**

The "Create Cisco Unity Voice Mailbox" link on the Directory Number Configuration window allows administrators to create individual Cisco Unity Connection voice mailboxes from Cisco Unified Communications Manager Administration. If Cisco Unified Communications Manager is integrated with Cisco Unity Connection, this link allows you to create a Cisco Unity Connection voice mailbox.

To configure a voice mailbox and other Cisco Unity Connection settings in Cisco Unity Connection Administration, see the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. Ensure that you have defined an appropriate template and selected a class of service (COS) for the users that you plan to add.

---

**Note**

Before you can create a Cisco Unity Connection voice mailbox for the end user, you must first configure the end user with a phone device association and a primary extension, and the integration between Cisco Unified Communications Manager and Cisco Unity Connection must be complete. For more information, see the Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection or the Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection.

---

**Before You Begin**

- You must configure Cisco Unified Communications Manager for voice-messaging service. See topics related to Cisco Unity and Cisco Unity Connection Configuration in the *Cisco Unified Communications Manager System Guide*.

- You must configure Cisco Unity Connection servers. See the applicable *Installation Guide for Cisco Unity Connection*.

- For Cisco Unity Connection integration, create an AXL connection via Cisco Unity Connection, as described in the "Managing the Phone System Integrations" chapter in the *System Administration Guide for Cisco Unity Connection*.

- Ensure the Cisco RIS Data Collector service is activated. See the *Cisco Unified Serviceability Administration Guide*. 
• On the Directory Number configuration window, ensure the Voice Mail Profile setting is configured and contains a pilot number, or the Voice Mail Profile setting should be set to None. If the Voice Mail Profile is set to No Voice Mail, the “Create Cisco Unity User” link does not display.

• Ensure that you have defined an appropriate template and selected a class of service (COS) for the users you plan to add. For Cisco Unity Connection users, see the User Moves, Adds, and Changes Guide for Cisco Unity Connection.

---

**Note**

The End User Configuration window also includes the “Create Cisco Unity Voice Mailbox” link.

---

**Procedure**

**Step 1** Choose **Call Routing > Directory Number** and click Add New.

**Step 2** Enter the appropriate settings in **Table 46: Directory number settings, on page 265**.

**Step 3** From the Related Links drop-down list box, in the upper, right corner of the window, choose the "Create Cisco Unity Voice Mailbox" link and click Go.

The Add Cisco Unity User dialog box displays.

**Step 4** From the Application Server drop-down list box, choose the Cisco Unity Connection server on which you want to create a Cisco Unity Connection mailbox and click Next.

**Step 5** From the Subscriber Template drop-down list box, choose the subscriber template that you want to use.

**Step 6** Click Save.

The Cisco Unity Connection mailbox gets created.

From Cisco Unity Connection Administration, you can now see the mailbox that you created. See the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection.

---

**Related Topics**

Directory number setup, on page 263
Meet-Me number and pattern setup

This chapter provides information about Meet-Me Number and Pattern configuration. For additional information, see topics related to conference bridges in the Cisco Unified Communications Manager System Guide.

- About Meet-Me number and pattern setup, page 297
- Meet-Me number and pattern settings, page 297

About Meet-Me number and pattern setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Meet-Me Number/Pattern menu path to configure meet-me numbers/patterns.

Meet-Me conferences require an allocation of directory numbers. Cisco Unified Communications Manager Administration provides the Meet-Me conference directory number range to users, so they can access the feature.

Meet-Me numbers and patterns configuration tips

Make sure that the following prerequisites are met before you configure Meet-Me numbers/patterns:

- Configure the server(s).
- Configure the device pools.

Related Topics

- Server setup, on page 25
- Device pool setup, on page 63

Meet-Me number and pattern settings

The following table describes the meet-me number/pattern settings.
**Table 47: Meet-Me number and pattern settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number or Pattern</td>
<td>Enter a Meet-Me Numbers/pattern or a range of numbers. To configure a range, the dash must appear within brackets and follow a digit; for example, to configure the range 1000 to 1050, enter 10[0-5]0.</td>
<td>To set the maximum list box items, choose System &gt; Enterprise Parameters and update the Max List Box Items field under CCMAdmin Parameters. Make sure that the combination of meet-me number/pattern and partition is unique within the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>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>
<td></td>
</tr>
<tr>
<td>Partition</td>
<td>To use a partition to restrict access to the meet-me/number pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the meet-me number/pattern, choose &lt;None&gt; for the partition. See the Partition setup, on page 241 for more information. 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. Find and choose a partition name by using the procedure in the Search for partition, on page 244.</td>
<td></td>
</tr>
<tr>
<td>Minimum Security Level</td>
<td>Choose the minimum Meet-Me conference security level for this meet-me number or pattern from the drop-down list box.</td>
<td>To invoke this feature, ensure you have a secure conference bridge that is configured and available. See the Cisco Unified Communications Manager Security Guide for more information.</td>
</tr>
<tr>
<td></td>
<td>• Choose Authenticated to block participants with nonsecure phones from joining the conference.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Choose Encrypted to block participants with authenticated or nonsecure phones from joining the conference.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Choose Non Secure to allow all participants to join the conference.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

Meet-Me number and pattern setup, on page 297
This chapter describes how to install, upgrade, or uninstall dial plans on Cisco Unified Communications Manager.

- **Dial plan setup, page 299**
- **Edit dial plan, page 299**
- **Restart Cisco CallManager service, page 303**

### Dial plan setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Dial Plan** Installer menu path to configure dial plans.

You can install a Cisco International Dial Plan and use it to create a unique numbering plan that is specific to a country, other than one in North America. Cisco Unified Communications Manager provides North American Numbering Plan (NANP) by default. Because dial plan requirements of other countries are unique to those countries, the default NANP configuration may not be the best suited configuration to create a dial plan for those countries. Cisco International Dial Plan allows you to create and update unique dial plans and make them available for use to Cisco customers worldwide.

Before you install a dial plan on the server, you should download the equivalent dial plan COP (Cisco Option Package) file to the Cisco Unified Communications Manager server.

You can find COP files for all the available dial plans that you can download, install, and integrate with Cisco Unified Communications Manager systems on the Cisco website.

For details on installing a COP file, see the *Cisco Unified Communications Manager Dial Plan Guide*.

**Related Topics**

- Install dial plan on Cisco Unified Communications Manager, on page 300

### Edit dial plan

Use the following procedures to install, upgrade, or uninstall dial plans.
Procedure

**Step 1** Find the Dial Plan that you want to install.

**Step 2** From the list of records, click the Dial Plan name that matches your search criteria. The Dial Plan Configuration window displays.

**Step 3** Complete one of the following tasks:
   a) Install a dial plan.
   b) Upgrade a dial plan.
   c) Uninstall a dial plan.

**Related Topics**

- Dial plan installer, on page 299
- Install dial plan on Cisco Unified Communications Manager, on page 300
- Upgrade dial plan, on page 301
- Uninstall dial plan, on page 302

**Install dial plan on Cisco Unified Communications Manager**

After you find a dial plan to install, use the following procedure to install the dial plan.

In the Dial Plan Configuration window, the dial plan name and description display in the Dial Plan and Description fields.

The Installed Version displays the current version that is installed on Cisco Unified Communications Manager server. If no version of the dial plan is installed, the Installed Version displays Not Installed.

**Procedure**

**Step 1** Choose the dial plan version that you want to install from the Available Version drop-down list box.

**Step 2** Click Install.

The Status displays that the dial plan has been installed.

The Installed Version field displays the dial plan version that is installed on Cisco Unified Communications Manager server.

**Step 3** Repeat Install dial plan on Cisco Unified Communications Manager, on page 300 to Install dial plan on Cisco Unified Communications Manager, on page 300 to install the dial plans on all the nodes Cisco Unified Communications Manager cluster.

**What to Do Next**

After installation of the dial plans, restart the Cisco CallManager service to load the dial plan.
Set up route pattern details for non-NANP dial plan

If you have installed a non-NANP dial plan on your Cisco Unified Communications Manager system, you can choose the required dial plan when you set up route pattern details in the Route Details Configuration window in Cisco Unified Communications Manager.

Note the following points when you configure route pattern details:

1. For a non-NANP dial plan, if you want to retain the settings at the Route Pattern level, make one of the following choices in the Route Details Configuration window:
   - Choose None in the Discard Digits field. Choosing None DDI in the Discard Digits field represents the same as not choosing a dial plan.
   - Choose a non-NANP dial plan: No Digits in the Discard Digits field. (For example, AMNP: No Digits.)

2. If you want to specify settings at the Route Group level that will override the Route Pattern settings, choose the appropriate DDI for that dial plan from the Discard Digits field. Examples of DDI: NANP: PreDot, AMNP: PreDot.

Upgrade dial plan

If you have installed a non-NANP dial plan, you can upgrade the dial plan that is installed on your Cisco Unified Communications Manager system with an upgraded version of the dial plan.

Caution
Upgrading a dial plan will fail if you configured one or more tags as a clause for a route filter in the existing version of the dial plan and the upgrade version does not contain these tags. After you upgrade to the new dial plan, the upgrade will list all such tags. You need to disassociate these tags from the route filter and run the dial plan upgrade again on the Cisco Unified Communications Manager system.

Caution
Upgrading a dial plan will fail if you have associated one or more DDIs with Route Patterns/Translation Patterns/Route Lists in the existing version of the dial plan and the upgrade version does not contain these DDIs. The dial plan upgrade will list all such DDIs. You need to disassociate these DDIs from Route Patterns/Translation Patterns/Route Lists and run the dial plan upgrade again on the Cisco Unified Communications Manager system.

Note
Make sure that you update the dial plans on the first node server of the Cisco Unified Communications Manager cluster before updating them on subscribers or other nodes in the cluster.

After you find a dial plan to upgrade, use the following procedure to upgrade an existing dial plan.
In the Dial Plan Configuration window, the dial plan name and description display in the Dial Plan and Description fields.

The Installed Version displays the current version that is installed on Cisco Unified Communications Manager server. If no version of the dial plan is installed, the Installed Version displays Not Installed.

**Procedure**

**Step 1** Choose the dial plan version that you want to upgrade from the Available Version drop-down list box.

**Step 2** Click Install. The Status displays that the dial plan has been upgraded. The Installed Version field displays the latest dial plan version.

**Step 3** Repeat **Step 1, on page 302 to Step 2, on page 302** to upgrade the dial plans on all nodes of Cisco Unified Communications Manager cluster where the Cisco CallManager service is installed.

**Note** After upgrading the dial plans, restart the Cisco CallManager service for the changes to take effect.

**Note** To update dial plans, you must install the COP file, as described in the Cisco Unified Communications Manager Dial Plan Guide, and install the dial plans that you want.

**Related Topics**

- Dial plan installer, on page 299
- Install dial plan on Cisco Unified Communications Manager, on page 300
- Restart Cisco CallManager service, on page 303

## Uninstall dial plan

**Caution** Before you uninstall a dial plan, ensure that you remove the route patterns, translation patterns, route lists, and route filters that are configured in the dial plan on the Cisco Unified Communications Manager system.

After you find a dial plan to uninstall, use the following procedure to uninstall the dial plan.

The dial plan name and description display in the Dial Plan and Description fields. The Installed Version displays the current version that is installed on the Cisco Unified Communications Manager server.

**Procedure**

**Step 1** Click Uninstall.

**Note** Dial plans should be uninstalled first from the first node in the cluster and then from the subsequent nodes. The Status displays that the dial plan was deleted. The Installed Version field displays Not Installed.
Step 2 Repeat Step 1, on page 302 to uninstall the dial plans on all nodes of the Cisco Unified Communications Manager cluster.

**Related Topics**

Dial plan installer, on page 299

---

**Restart Cisco CallManager service**

Use the following procedure to restart the Cisco CallManager service.

**Procedure**

**Step 1** In the Cisco Unified Serviceability window, choose Tools > Control Center - Feature Services. The Control Center–Feature Services window displays.

**Step 2** Choose the Cisco Unified Communications Manager server from the Servers drop-down list box. In the CM Services area, Cisco CallManager displays in the Service Name column.

**Note** Click the radio button corresponding to the Cisco CallManager service.

**Step 3** If you want to restart the Cisco CallManager service, click Restart. The service restarts, and the message, Service Successfully Restarted, displays.

**Step 4** If you want to start a stopped Cisco CallManager service, click Start. The service starts, and the message, Service Successfully Started, displays.

**Related Topics**

Dial plan installer, on page 299
Route plan report

This chapter provides information about viewing route plan report records and managing unassigned directory numbers.

For additional information, see topics related to route plans and directory number configuration settings in the Cisco Unified Communications Manager System Guide. Also see topics related to local route groups in the Cisco Unified Communications Manager Features and Services Guide.

- About route plan report, page 305
- View route plan records, page 306
- Delete unassigned directory number, page 307
- Update unassigned directory numbers, page 308
- View route plan reports in files, page 308

About route plan report

The route plan report lists all of the following types of directory and other numbers in the system:

- Unassigned directory numbers (DN)
- Call park numbers
- Conference numbers
- Directory numbers (DN)
- Calling party transformation patterns
- Called party transformation patterns
- Translation patterns
- Call pickup group numbers
- Route patterns
- Message-waiting indicators
- Voice-mail ports
• Domain routing
• IP routing
• Hunt pilots
• Directed call park numbers
• Intercom directory numbers
• Intercom translation patterns
• Handoff numbers (configured in the Mobility Configuration window [Call Routing > Mobility > Handoff Configuration])
• Enterprise Feature Access numbers (configured in the Mobility Configuration window [Call Routing > Mobility > Enterprise Feature Access Configuration])
• Mobile Voice Access numbers (configured in the Service Parameters window [System > Service Parameters])
• Mobile Voice Access directory numbers (configured in the Mobile Voice Access window [Media Resources > Mobile Voice Access])

The route plan report allows you to view either a partial or full list and to go directly to the associated configuration windows by clicking the entry in the Pattern/Directory Number, Partition, or Route Detail columns of the report.

In addition, the route plan report allows you to save report data into a .csv file that you can import into other applications. The .csv file contains more detailed information than the web pages, including directory numbers for phones, route patterns, pattern usage, device name, and device description.

Cisco Unified Communications Manager uses the route plan to route both internal calls and external public switched telephone network (PSTN) calls. For more detailed information on the route plan, see topics related to understanding route plans in Cisco Unified Communications Manager System Guide.

Note
See topics related to local route groups in the Cisco Unified Communications Manager System Guide for a discussion of the route plan report and its format when the Local Route Group feature is configured.

Related Topics
   Route plan report, on page 305
   View route plan records, on page 306
   Delete unassigned directory number, on page 307
   View route plan reports in files, on page 308

View route plan records

This section describes how to view route plan records. Because you might have several records in your network, Cisco Unified Communications Manager Administration lets you locate specific route plan records on the basis of specific criteria. Use the following procedure to generate customized route plan reports.
Procedures

**Step 1** Choose Call Routing > Route Plan Report.
The Route Plan Report window displays.

**Step 2**
To find all records in the database, ensure the dialog box is empty; go to **Step 3, on page 307**.
To filter or search records:
1) From the first drop-down list box, select a search parameter.
2) From the second drop-down list box, select a search pattern.
3) Specify the appropriate search text, if applicable.

**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.
The window displays the item that you choose.

**Related Topics**
Route plan report, on page 305

Delete unassigned directory number

This section describes how to delete an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified Communications Manager Administration. When a directory number gets removed from a device or a phone gets deleted, the directory number still exists in the Cisco Unified Communications Manager database. To delete the directory number from the database, use the Route Plan Report window.

Procedures

**Step 1** Choose Call Call Routing > Route Plan Report.
The Route Plan Report window displays. Use the three drop-down list boxes to specify a route plan report that lists all unassigned DNs.

**Step 2**
Three ways exist to delete directory numbers:
1) Click the directory number that you want to delete. When the Directory Number Configuration window displays, click Delete.
2) Check the check box next to the directory number that you want to delete. Click Delete Selected.
3) To delete all found unassigned directory numbers, click Delete All Found Items.
   A warning message verifies that you want to delete the directory number.

**Step 3**
To delete the directory number, click OK. To cancel the delete request, click Cancel.
Update unassigned directory numbers

This section describes how to update the settings of an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified Communications Manager Administration. When a directory number gets removed from a device, the directory number still exists in the Cisco Unified Communications Manager database. To update the settings of the directory number, use the Route Plan Report window.

Procedure

**Step 1**  Choose **Call Routing > Route Plan Report**. The Route Plan Report window displays. Use the three drop-down list boxes to specify a route plan report that lists all unassigned DNs.

**Step 2**  Click the directory number that you want to update. The Directory Number Configuration window displays.

**Note**  You can update all the settings of the directory number except the directory number and partition.

**Step 3**  Make the required updates such as calling search space or forwarding options.

**Step 4**  Click Save. The Directory Number Configuration window redisplays, and the directory number field is blank.

View route plan reports in files

This section contains information on how to view route plan reports in a .csv file.

Procedure

**Step 1**  Choose **Call Routing > Route Plan Report**. The Route Plan Report window displays.

**Step 2**  Choose View In File from the Related Links drop-down list box on the Route Plan Report window and click Go. A dialog box displays. From this dialog box, you can either save the file or import it into another application.

**Step 3**  Click Save. Another window displays that allows you to save this file to a location of your choice.

**Note**  You may also save the file as a different file name, but the file name must include a .csv extension.
Step 4  Choose the location in which to save the file and click Save. This action should save the file to the location that you designated.

Step 5  Locate the .csv file that you just saved and double-click its icon to view it.

View route plan reports in files
View route plan reports in files
CHAPTER 48

Calling party transformation pattern setup

This chapter provides information to find, add, update, copy, or delete a calling party transformation pattern. For additional information, see topics related to calling party number transformations settings, wildcards and special characters in route patterns and hunt pilots in the Cisco Unified Communications Manager System Guide. Also see topics related to calling party normalization and local route groups in the Cisco Unified Communications Manager Features and Services Guide.

- About calling party transformation pattern setup, page 311
- Calling party transformation pattern settings, page 311

About calling party transformation pattern setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Transformation Pattern > Calling Party Transformation Pattern menu path to configure calling party transformation patterns.

The parameters in the Calling Party Transformation Patterns window provide appropriate caller information using the Calling Party Transformation calling search space on the destination device. Be aware that calls through transformation patterns are not routable. When this pattern is matched, the call does not route to any device.

You use calling party transformation patterns with the calling party normalization feature. For information on the calling party normalization feature, see topics related to calling party normalization in the Cisco Unified Communications Manager Features and Services Guide.

Note

See topics related to local route groups in the Cisco Unified Communications Manager Features and Services Guide for a discussion of calling party transformation patterns and their use and configuration when the Local Route Group feature is configured.

Calling party transformation pattern settings

The following table describes the calling party transformation pattern settings.
### Calling party transformation pattern settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Pattern Definition** | Enter the transformation pattern, including numbers and wildcards (do not use spaces); for example, for NNP, 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 +.  
**Note** Ensure that the pattern is unique. Check the transformation pattern, route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report.  
See topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide* for more information about wildcards. |
| **Partition**     | If you want to use a partition to restrict access to the transformation pattern, choose the desired partition from the drop-down list box.  
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, then find and choose a partition name.  
**Note** Configure transformation patterns in different non-null partitions rather than dialing patterns such as route patterns and directory numbers. For transformation pattern lookups, Cisco Unified Communications Manager ignores the patterns in null partitions.  
**Note** To set the maximum list box items, choose *System > Enterprise Parameters* and choose CCMAadmin Parameters.  
**Note** Make sure that the combination of pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster. |
| **Description**   | Enter a description of the transformation pattern.                                                                                                                                                                                                                                                                                    |
| **Numbering Plan** | Choose a numbering plan.                                                                                                                                                                                                                                                                                                           |
| **Route Filter**  | If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns.  
The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.  
You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name.  
**Note** To set the maximum list box items, choose *System > Enterprise Parameters* and choose CCMAadmin Parameters. |

---

**Note** See topics related to wildcards and special characters in route patterns and hunt pilots in the *Cisco Unified Communications Manager System Guide* for more information about wildcards.
### Calling party transformation pattern settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgent Priority</td>
<td>Cisco Unified Communications Manager sets all calling party transformation patterns with urgent priority, and you cannot change the priority of the patterns.</td>
</tr>
<tr>
<td><strong>Calling Party Transformations</strong></td>
<td></td>
</tr>
<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. You may also configure an External Phone Number Mask on all phone devices.</td>
</tr>
<tr>
<td>Discard Digit Instructions</td>
<td>Choose the discard digit instructions that you want to be associated with this calling party transformation pattern. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.</td>
</tr>
</tbody>
</table>
| Calling Party Transform Mask        | Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); and the international escape character +.  
If the Discard Digit Instructions field is blank, the Prefix Digits (Outgoing Calls) field is blank, the Calling Party Transformation Mask field is blank, and the Use Calling Party's External Phone Number Mask is not checked, no calling party transformation takes place. |
| Prefix Digits (Outgoing Calls)      | Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries include the digits 0 through 9, the wildcard characters asterisk (*) and octothorpe (#), and the international escape character +.  
**Note** The appended prefix digit does not affect which directory numbers route to the assigned device. |
| 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 route 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. |
## Calling Party Transformation Pattern Settings

<table>
<thead>
<tr>
<th>Field</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 type numbering plan. Choose one of the following options:  
  • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type.  
  • Unknown—Use 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. |
| Calling Party Numbering Plan | Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options:  
  • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.  
  • ISDN—Use when you are dialing outside the dialing plan for your country.  
  • National Standard—Use when you are dialing within the dialing plan for your country.  
  • Private—Use when you are dialing within a private network.  
  • Unknown—Use when the dialing plan is unknown. |

### Related Topics

- About route filter setup, on page 169  
- Partition setup, on page 241  
- Search for partition, on page 244  
- Calling party transformation pattern setup, on page 311
Called party transformation pattern setup

This chapter provides information to configure a called party transformation pattern. For additional information, see topics related to called party number transformations settings, wildcards and special characters in route patterns and hunt pilots in the Cisco Unified Communications Manager System Guide. Also see topics related to local route groups in the Cisco Unified Communications Manager Features and Services Guide.

• About called party transformation pattern setup, page 315
• Called party transformation pattern settings, page 315

About called party transformation pattern setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Transformation Pattern > Called Party Transformation Pattern menu path to configure called party transformation patterns.

The parameters in the Called Party Transformation Patterns window provide appropriate caller information by using the Called Party Transformation calling search space on the destination device. Be aware that calls through transformation patterns are not routable. When this pattern is matched, the call does not route to any device.

Note

See topics related to local route groups in the Cisco Unified Communications Manager Features and Services Guide for a discussion of called party transformation patterns and their use and configuration when the Local Route Group feature is configured.

Called party transformation pattern settings

The following table describes the called party transformation pattern settings.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern</td>
<td>Enter the transformation pattern, including numbers and wildcards (do not use spaces); for example, for NAP, enter 9.@ for typical local access, or 8XXX for a typical private network numbering plan. Valid characters include the uppercase letters A, B, C, and D and +, which represents the international escape character +. <strong>Note</strong> Ensure that the pattern is unique. Check the transformation pattern, route pattern, translation pattern, directory number, call park number, call pickup number, message waiting on/off, or meet me number if you receive an error that indicates duplicate entries. You can also check the route plan report. See topics related to wildcards and special characters in route patterns and hunt pilots in the <em>Cisco Unified Communications Manager System Guide</em> for more information about wildcards.</td>
</tr>
<tr>
<td>Partition</td>
<td>If you want to use a partition to restrict access to the transformation pattern, choose the desired partition from the drop-down list box. If you do not want to restrict access to the transformation pattern, choose &lt;None&gt; 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, then find and choose a partition name. <strong>Note</strong> Transformation patterns should be configured in different non- NULL partitions than dialing patterns such as route patterns and directory numbers. For transformation pattern lookups, the patterns in NULL partitions get ignored. <strong>Note</strong> To set the maximum list box items, choose <em>System &gt; Enterprise Parameters</em> and choose CCMAdmin Parameters. <strong>Note</strong> Make sure that the combination of pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the transformation pattern. 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>
<tr>
<td>Numbering Plan</td>
<td>Choose a numbering plan.</td>
</tr>
</tbody>
</table>

*Table 49: Called party transformation pattern settings*
If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns.

The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.

You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name.

**Note** To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Cisco Unified Communications Manager sets all called party transformation patterns with urgent priority, and you cannot change the priority of the patterns.

### Field | Description
--- | ---
Route Filter | If your transformation pattern includes the @ wildcard, you may choose a route filter. The optional act of choosing a route filter restricts certain number patterns.

The route filters that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.

You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more route filters 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 Route Filters window, then find and choose a route filter name.

**Note** To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

Urgent Priority | Cisco Unified Communications Manager sets all called party transformation patterns with urgent priority, and you cannot change the priority of the patterns.

Called Party Transformations

Discard Digits | Choose the discard digits instructions that you want to be associated with this called party transformation pattern. The discard digits that display depend on the numbering plan that you choose from the Numbering Plan drop-down list box.

Called Party Transform Mask | Enter a transformation mask value. Valid entries include the digits 0 through 9; the wildcard characters X, asterisk (*), and octothorpe (#); the international escape character +; and blank. If this field is blank and the preceding field is not checked, no transformation takes place.

Prefix Digits | Enter prefix digits in the Prefix Digits (Outgoing Calls) field. Valid entries 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 get routed to the assigned device.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called Party Number Type</td>
<td>Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called party directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NAPN 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 called directory number to be encoded to a non national type numbering plan. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Use when the dialing plan is unknown.</td>
</tr>
<tr>
<td></td>
<td>• National—Use when you are dialing within the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• International—Use when you are dialing outside the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.</td>
</tr>
<tr>
<td>Called Party Numbering Plan</td>
<td>Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NAPN 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 PBXs by using routing as a non national type number. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.</td>
</tr>
<tr>
<td></td>
<td>• ISDN—Use when you are dialing outside the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• National Standard—Use when you are dialing within the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• Private—Use when you are dialing within a private network.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Use when the dialing plan is unknown.</td>
</tr>
</tbody>
</table>

**Related Topics**

- About route filter setup, on page 169
- Partition setup, on page 241
- Search for partition, on page 244
- Called party transformation pattern setup, on page 315
Intercluster directory URI settings

In Cisco Unified CM Administration, use the Call Routing > Intercluster Directory URI > Intercluster Directory URI Configuration path to enable ILS support for URI dialing across clusters. After you configure URI dialing in the local cluster you can configure the settings on this page to expand URI dialing support across clusters.

Configuration Tips

Before you configure the settings on this page, you must do the following:

• Set up URI dialing in the local cluster. See the URI dialing chapter of the Cisco Unified Communications Manager System Guide for more information.

• Set up an ILS network. See the Intercluster Lookup Service chapter of the Cisco Unified Communications Manager Features and Services Guide for more information.

The following table describes the settings in the Intercluster Directory URI Configuration window.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Exchange Directory URI Catalogs with Remote Clusters | Check this check box to enable the URI Replication feature with ILS. When this check box is checked, the local cluster sends its directory URIs and route strings to remote clusters in the ILS network and also receives directory URI catalogs and route strings from the remote clusters in the ILS network.  
If this check box is checked for all clusters in the ILS network, each cluster in the network learns the directory URIs and route strings for all the other clusters in the network.  
**Note** You must check this check box if you want to implement URI dialing across clusters.                                                                                      |
| Route String                                    | Enter a route string for this cluster. Route strings can be up to 250 alphanumeric characters and can include dots and dashes. Route strings must have at least one dot.  
If the Exchange Directory URI Catalogs with Remote Clusters check box is checked, the local cluster includes its route string when it exchanges directory URI catalogs with remote clusters in the ILS network.  
When a remote cluster in the ILS network receives a call that is addressed to a directory URI in this cluster, the remote cluster pulls the route string for this cluster.  
If a route pattern is configured that matches the route string, the remote cluster sends the call to the outbound trunk that is specified by the route pattern.  
**Note** In order for Cisco Unified Communications Manager to route calls to a route string, you must configure SIP route patterns that match the route string and point those SIP route patterns to an outbound trunk that routes to that cluster.  
See the Sip route pattern setup chapter of the *Cisco Unified Communications Manager Administration Guide* for more information on SIP route patterns. |
| Export Local Directory URIs                     | Click this button to export all directory URIs that were configured in the local cluster, including directory URIs that were imported from an LDAP directory, to a CSV export file. The export file can be imported into another call control system that is not running ILS such as a Cisco TelePresence Video Communication Server.  
**Note** The export file does not contain directory URIs that were learned by ILS or directory URIs that were manually imported from another system. |
The local cluster must be a hub cluster in an existing ILS network. For more information on ILS networks, see the Intercluster Lookup Service chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

The following table contains field descriptions for the Imported Directory URI Catalog window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name to identify the imported directory URI catalog that you want to import.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the directory URI catalog that you want to import.</td>
</tr>
<tr>
<td>Route String</td>
<td>Enter a route string for the remote call control system. Route strings can be up to 250 alphanumeric characters long and can include dots and dashes. Cisco Unified Communications Manager uses route strings in conjunction with SIP route patterns to route calls to directory URIs that are configured in remote clusters. When a call from the local cluster is placed to a directory URI in this remote catalog, Cisco Unified Communications Manager matches the directory URI with the route string and then uses a SIP route pattern to match that route string to an outbound trunk that routes to that directory URI. Note: After you create the route string, create a SIP route pattern that routes this route string to an outbound trunk. See the SIP route pattern setup chapter of the <em>Cisco Unified Communications Manager Administration Guide</em> for more information on SIP route patterns.</td>
</tr>
</tbody>
</table>

**Related Topics**

Import Directory URIs from a non-ILS system, on page 322

**Find imported directory URIs**

**Procedure**

Select Call Routing > Intercluster Directory URI > Imported Directory URIs to display a list of imported directory URI catalogs, in Cisco Unified CM Administration.

The Find and List Imported Directory URIs window displays a complete list of directory URIs that were manually imported from another call control system, along with a corresponding directory URI catalog.

**Note**

The Find and List Imported Directory URIs window displays only those directory URIs and directory URI catalogs that were manually imported into the local Cisco Unified Communications Manager cluster from another call control system. This window does not display directory URIs that were configured locally in Cisco Unified CM Administration, directory URIs that were imported from a corporate LDAP directory, or directory URIs that were learned by the Intercluster Lookup Service.
Import Directory URIs from a non-ILS system

Follow this procedure if you are running the Intercluster Lookup Service (ILS) on your local cluster and you want to import directory URIs from a CSV file for a call control system that is not running ILS, such as a Cisco TelePresence Video Communication Server (VCS), or a third-party call control system.

To perform this procedure, the Cisco Bulk Provisioning Service must be running on the local cluster, which must be configured as a hub cluster in an ILS network. After you import the catalog into Cisco Unified Communications Manager, ILS replicates the imported catalog to the other clusters in the ILS network.

Note

Within Cisco Unified CM Administration, you can enter directory URIs with embedded double quotes or commas. However, when you use Bulk Administration to import a CSV file that contains directory URIs with embedded double quotes and commas, you must use enclose the entire directory URI in double quotes and escape the embedded double quotes with a double quote. For example, a directory URI of Jared,"Jerry",Smith@test.com must be input as "Jared,""Jerry"",Smith@test.com" in the CSV file.

Procedure

Step 1 In Cisco Unified CM Administration, choose Call Routing > Intercluster Directory URIs > Imported Directory URI Catalogs.
Step 2 In the Name field, enter a name for the directory URI catalog.
Step 3 In the Description field, enter a description of the directory URI catalog.
Step 4 In the Route String field, create a route string for the system from which you are importing the URI catalog.
Step 5 Click Save.
Step 6 In Cisco Unified CM Administration, choose Bulk Administration > Upload/Download Files.
Step 7 Click Add New.
Step 8 Click Browse and select the CSV file for the directory URI catalog that you want to import.
Step 9 In the Select the Target drop-down list box, choose Imported Directory URIs.
Step 10 In the Select Transaction Type drop-down list box, choose Insert Imported Directory URIs.
Step 11 Click Save.
Step 12 In Cisco Unified CM Administration, choose Bulk Administration > Imported Directory URIs > Insert Imported Directory URIs.
Step 13 In the File Name drop-down list box, choose the CSV file that contains the imported directory URI catalog.
Step 14 In the Imported Directory URI Catalog drop-down list box, choose the directory URI catalog that you named in the Imported Directory URI Catalog window.
Step 15 In the Job Description text box, enter a name for the job that you are about to run.
Step 16 Select when you want to run the job.

• If you want to run the job now, click the Run Immediately radio button, and click Submit.
If you want to schedule the job to run at a specified time, check the Run Later radio button and click Submit. If you choose this option, you must use the Bulk Administration Job Scheduler to schedule when the job runs.

### Directory URI format

Directory URIs are alphanumeric strings consisting of a user and a host address separated by the @ symbol. Cisco Unified Communications Manager supports the following formats for directory URIs:

- **user@domain** (for example, joe@cisco.com)
- **user@ip_address** (for example, joe@10.10.10.1)

Cisco Unified Communications Manager supports the following formats in the user portion of a directory URI (the portion before the @ symbol):

- Accepted characters are a-z, A-Z, 0-9, $, %, &, , _ , + , ~ , = , \ , ? , , . , / .
- The user portion has a maximum length of 47 characters.
- The user portion accepts percent encoding from %2[0-9A-F] through %7[0-9A-F]. For some accepted characters, Unified CM automatically applies percent encoding. See below for more information on percent encoding.
- The user portion is case-sensitive or case-insensitive depending on the value of the URI Lookup Policy enterprise parameter. The default value is case-sensitive.

Cisco Unified Communications Manager supports the following formats in the host portion of a directory URI (the portion after the @ symbol):

- Supports IPv4 addresses or fully qualified domain names.
- Accepted characters are a-z, A-Z , 0-9 , hyphens, and dots.
- The host portion cannot start or end with a hyphen.
- The host portion cannot have two dots in a row.
- Minimum of two characters.
- The host portion is not case sensitive.

Due to database restrictions, the Directory URI field has a maximum length of 254 characters.

---

**Note**

You can also enter a directory number in the user portion of a directory URI. However, Cisco Unified Communications Manager may treat the directory URI as a directory number depending on which Dial String Interpretation option you choose for the SIP Profile.
For compatibility with third party call control systems, Cisco recommends setting the value of the URI Lookup Policy enterprise parameter to case insensitive.

Note

Percent encoding of directory URIs
In the user portion of a directory URI, Unified CM automatically applies percent encoding to the following characters when the directory URI is saved in the database:

# % ^ ` { } \ : " < > [ ] \ and spaces

When percent encoding is applied, the digit length of the directory URI increases. For example, if you input joesmith#@cisco.com (20 characters) as a directory URI, Cisco Unified Communications Manager stores the directory URI in the database as joe%20smith%23@cisco.com (24 characters). Due to database restrictions, Cisco Unified Communications Manager rejects any attempt to save a directory URI of greater than 254 characters.

Directory URI format exception for Bulk Administration
Within Cisco Unified CM Administration, you can enter directory URIs with embedded double quotes or commas. However, when you use Bulk Administration to import a CSV file that contains directory URIs with embedded double quotes and commas, you must use enclose the entire directory URI in double quotes and escape the embedded double quotes with a double quote. For example, the Jared,”Jerry”,Smith@test.com directory URI must be input as "Jared,""Jerry"",Smith@test.com" in the CSV file.
Other call routing menu options

This chapter provide brief descriptions of selected Call Routing menu options. A pointer to documents that contain a more detailed description for each of these Call Routing menu options is provided.

- Intercom partition setup, page 325
- Intercom calling search space setup, page 326
- Intercom directory number setup, page 326
- Intercom translation pattern setup, page 326
- Access list setup, page 326
- Client Matter Code setup, page 327
- Forced Authorization Code setup, page 327
- Call Park setup, page 327
- Directed Call Park setup, page 328
- Call Pickup Group setup, page 328
- Transformation profile setup, page 329
- Mobility setup, page 329
- Logical partitioning policy setup, page 329
- Call control discovery setup, page 330
- External call control profile setup, page 330

Intercom partition setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Intercom > Intercom Route Partition menu path to configure intercom partitions.

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 the Cisco Unified Communications Manager System Guide.
For more information about intercom partitions, see the Cisco Unified Communications Manager System Guide.

**Intercom calling search space setup**

In Cisco Unified Communications Manager Administration, use the Call Routing > Intercom > Intercom Calling Search Space menu path to configure intercom calling search spaces.

An intercom calling search space comprises an ordered list of intercom calling search spaces 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 the Cisco Unified Communications Manager System Guide. For more information about intercom and intercom calling search spaces, see the Cisco Unified Communications Manager System Guide.

**Intercom directory number setup**

In Cisco Unified Communications Manager Administration, use the Call Routing > Intercom > Intercom Directory Number menu path to configure intercom directory numbers.

Using Cisco Unified Communications Manager Administration, configure and modify intercom directory numbers (DNs) that are assigned to specific phones.

For more information on how to configure intercom directory numbers, see the Cisco Unified Communications Manager System Guide.

**Intercom translation pattern setup**

In Cisco Unified Communications Manager Administration, use the Call Routing > Intercom > Intercom Translation Pattern menu path to configure intercom translation patterns.

Cisco Unified Communications Manager uses 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.

For more information on how to configure intercom translation patterns, see the Cisco Unified Communications Manager System Guide.

**Access list setup**

In Cisco Unified Communications Manager Administration, use the Call Routing > Class of Control > Access List menu path to configure access lists.

Mobile Connect allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Access lists determine the phone numbers that are explicitly allowed or blocked for in-progress call transfers.

For more information on Mobile Connect and how to configure access lists, see the Cisco Unified Communications Manager System Guide.
Client Matter Code setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Client Matter Codes menu path to configure client matter codes.

Client Matter Codes (CMC) assist with call accounting and billing for billable clients. CMC 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 CMC feature requires that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled CMC for each route pattern. You can access the Client Matter Codes search and configuration windows from Call Routing > Client Matter Codes in Cisco Unified Communications Manager Administration.

For detailed information about client matter codes, see the Cisco Unified Communications Manager System Guide.

Additional Cisco Documentation
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Serviceability Administration Guide

Forced Authorization Code setup

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. This feature regulates the types of calls that certain users can place by forcing the user to enter a valid authorization code before the call completes.

The FAC feature requires that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled FAC for each route pattern. You can access the Forced Authorization Code search and configuration windows from Call Routing > Forced Authorization Codes in Cisco Unified Communications Manager Administration.

For detailed information about forced authorization codes, see the Cisco Unified Communications Manager System Guide.

Additional Cisco Documentation
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Serviceability Administration Guide

Call Park setup

In Cisco Unified Communications Manager Administration, use the Call Routing > Call Park menu path to configure call park numbers.
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.

For more information on how to use and configure the Call Park feature, see the *Cisco Unified Communications Manager System Guide*.

### Directed Call Park setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Directed Call Park** menu path to configure directed call park numbers.

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.

A user can retrieve a parked call by dialing a configured retrieval prefix followed by the directed call park number where the call is parked.

For more information on how to use and configure the directed call park feature, see the *Cisco Unified Communications Manager System Guide*.

### Call Pickup Group setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Call Pickup Group** menu path to configure call pickup groups.

The Call Pickup Group menu option allows administrators to configure call pickup groups. After end users are configured as members of a call pickup group, these users can answer a call that comes in on a directory number other than their own. When a user hears an incoming call ringing on another phone, the user can redirect the call to their own phone by using one of the call pickup phone features.

Cisco Unified IP Phones that are running SCCP and SIP provide several types of 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 a user activates this feature on a phone.

- 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 they activate this feature on a phone.

- The Other Group Pickup feature allows users to pick up incoming calls in a group that is associated with their own group. When a phone rings in a group that is associated with the user group, Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups when they activate this feature on a phone.

- The Directed Call Pickup feature allows a user to pick up an incoming call on a directory number (DN) directly by pressing the GPickUp softkey and entering the directory number.

- The Busy Lamp Field (BLF) Call Pickup feature allows a user to pick up a call that is directed to the DN that is associated with the BLF button that is configured on the user Cisco Unified IP Phone.
Transformation profile setup

Cisco Intercompany Media Engine configuration comprises configuration of transformation profiles. For more information, see the Cisco Intercompany Media Engine Installation and Configuration Guide.

Mobility setup

In Cisco Unified Communications Manager Administration, use the following menu paths to configure Cisco Unified Mobility configuration:

- **Call Routing > Mobility > Enterprise Feature Access Configuration**
- **Call Routing > Mobility > Handoff Configuration**
  - Call Routing > Mobility > Handoff Configuration
- **Call Routing > Mobility > Mobility Profile**

Mobile Connect allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. The Mobility Configuration window contains dual mode phone handoff settings for call transfers between a user desktop phone and mobile phone.

The Enterprise Feature Access Configuration window allows you to configure the Enterprise Feature Access (EFA) number for Cisco Unified Mobility calls.

The Handoff Mobility Configuration window allows you to configure the handoff number that the system uses to hand off Cisco Unified Mobility calls.

The Mobility Profile Configuration window allows you to configure mobility profiles for Cisco Unified Mobility users. The mobility profile of a user determines whether user mobility calls use the Dial-via-Office Forward or Dial-via-Office Reverse Callback feature for mobility calls.

For more information on Mobile Connect and how to configure mobility settings for dual-mode phones, see the Cisco Unified Communications Manager System Guide.

Logical partitioning policy setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Logical Partitioning Policy Configuration** menu path to configure logical partitioning policies.

You use logical partitioning policies with geographic locations and geographic location filters to provision logical partitioning.

For more information on how to use the Logical Partitioning Policy Configuration window, see the Cisco Unified Communications Manager System Guide.
Call control discovery setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > Call Control Discovery > Feature Configuration** menu path to configure call control discovery feature parameters.

External call control profile setup

In Cisco Unified Communications Manager Administration, use the **Call Routing > External Call Control Profile** menu path to configure external call control profiles.
PART IV

Media resource setup

• Annunciator setup, page 333
• Conference Bridge setup, page 337
• Media termination point setup, page 363
• Transcoder setup, page 367
• Media resource group setup, page 371
• Media resource group list setup, page 375
• Announcement setup, page 377
• Other media resource menu options, page 383
Annunciator setup

This chapter provides information to find and update annunciators. For additional information, see topics related to annunciators and trusted relay points in the Cisco Unified Communications Manager System Guide. Also see topics related to multilevel precedence and preemption in the Cisco Unified Communications Manager Features and Services Guide.

- About annunciator setup, page 333
- Annunciator deletion, page 334
- Annunciator settings, page 334
- Synchronize annunciators, page 336

About annunciator setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Annunciator menu path to configure annunciators.

An annunciator, an SCCP device that uses the Cisco Media Streaming Application service, enables Cisco Unified Communications Manager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones and gateways. The annunciator, which works with Cisco Multilevel Precedence and Preemption (MLPP), enables Cisco Unified Communications Manager to alert callers as to why the call fails. Annunciator can also play tones for some transferred calls and some conferences.

Annunciator configuration tips

Verify that you have activated the Cisco IP Voice Media Streaming Application service on the server where you plan to configure the annunciator. For information on activating services, see the Cisco Unified Serviceability Administration Guide.

Tip

When you add a Cisco Unified Communications Manager server, the annunciator for the sever automatically gets added to the database. After you activate the Cisco IP Voice Media Streaming Application service, the annunciator device registers with Cisco Unified Communications Manager.

Before you begin to configure an annunciator, verify that you have completed the following tasks:
• Configured the appropriate servers
• Configured device pools

Related Topics
  Synchronize annunciators, on page 336

Annunciator deletion

You cannot delete an annunciator if other devices are using it. If you find that any devices are using the annunciator that you want to delete, you must first update those devices to use a different annunciator.

To find which devices are using the annunciator, choose Dependency Records from the Related Links drop-down list menu and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Related Topics
  Access dependency records, on page 874

Annunciator settings

The following table describes the annunciator settings.

Table 51: Annunciator settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The system automatically displays the preconfigured server (servers get added at installation).</td>
</tr>
<tr>
<td>Name</td>
<td>This field designates the name that is used when the device registers with the Cisco Unified Communications Manager. Enter a name of up to 15 alphanumeric characters (you can use periods, dashes, and underscores).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of up to 128 alphanumeric characters (you can use periods, dashes, and underscores). Default uses the server name, which includes the prefix ANN_.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose Default or choose a device pool from the drop-down list of configured device pools.</td>
</tr>
</tbody>
</table>
Use locationsto implement call admission control (CAC) in a centralized call-processing system. CAC allows you to regulate audio quality and video availability by limiting the 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 annunciator.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this annunciator consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the System > Location menu option.

For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.

<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 allows you to regulate audio quality and video availability by limiting the 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 annunciator. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this annunciator consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the System &gt; Location menu option. For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Use Trusted Relay Point</td>
<td>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 RSVP Agent). If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. For details of call behavior, see Cisco Unified Communications Manager System Guide. If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVP Agent 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 Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.</td>
</tr>
</tbody>
</table>

**Related Topics**

Location setup, on page 107
Annunciator setup, on page 333
Synchronize annunciators

To synchronize an annunciator with the most recent configuration changes, perform the following procedure, which applies 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 Media Resources > Annunciator.
The Find and List Annunciators window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find.
The window displays a list of annunciators that match the search criteria.

**Step 4** Check the check boxes next to the annunciators that you want to synchronize. To choose all annunciators in the window, check the check box in the matching records title bar.

**Step 5** Click Apply Config to Selected.
The Apply Configuration Information dialog displays.

**Step 6** Click OK.

**Related Topics**

Annunciator setup, on page 333
Conference Bridge setup

This chapter provides information to configure conference bridges using Cisco Unified Communications Manager Administration.

See the following for additional information:

- Conference bridges and trusted relay points in the *Cisco Unified Communications Manager System Guide*
- Configuring Secure Conference Bridge in Cisco Unified Communications Manager Administration, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified Communications Manager Administration Guide for Cisco Business Edition 5000
- Configuring Secure Conference Bridge in Cisco Unified Communications Manager Administration, *Cisco Unified Communications Manager Security Guide*
- *Cisco Unified Videoconferencing 3511 MCU and Cisco Unified Videoconferencing 3540 MCU Module Administrator Guide*
- *Cisco Unified Serviceability Administration Guide*

- About conference bridge setup, page 337
- Conference Bridge deletion, page 338
- Conference Bridge settings, page 338
- Set up TLS connection with Cisco TelePresence MCU, page 360
- Synchronize conference device settings, page 361

About conference bridge setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Conference Bridge menu path to configure conference bridges.

Conference bridge configuration tips

Make sure that the following prerequisites are met before you proceed with configuration of a conference bridge:
• Configure the device pools.

**Note**  Software conference bridges automatically get created when the Cisco Unified Communications Manager server gets created. You cannot add software conference bridges to Cisco Unified Communications Manager Administration.

• For software conference bridges, activate the Cisco IP Voice Media Streaming Application service. See the *Cisco Unified Serviceability Administration Guide*.

**Related Topics**

- [Device pool deletion](#)
- [Software Conference Bridge settings](#)
- [Synchronize conference device settings](#)

### Conference Bridge deletion

Keep in mind that you cannot delete Cisco Unified Communications Manager Conference Bridge Software. Cisco Unified Communications Manager allows you to delete devices that may be associated with components such as media resource groups. To find out what dependencies the conference device may have, choose the Dependency Records link from the drop-down list box and click Go from the Conference Bridge Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

**Related Topics**

- [Conference Bridge setup](#)
- [Access dependency records](#)

### Conference Bridge settings

Consult the conference bridge configuration settings table that corresponds to the type of conference bridge that you are configuring.

**Related Topics**

- [Conference Bridge setup](#)
- [Software Conference Bridge settings](#)
- [Hardware Conference Bridge settings](#)
- [Cisco IOS Conference Bridge settings](#)
- [Cisco Video Conference Bridge settings](#)
- [Cisco Conference Bridge (WS-SVC-CMM) settings](#)
- [Cisco IOS Heterogeneous Video Conference Bridge settings](#)
- [Cisco IOS Guaranteed Audio Video Conference Bridge settings](#)
- [Cisco IOS Homogeneous Video Conference Bridge settings](#)
- [Cisco TelePresence MCU settings](#)
Software Conference Bridge settings

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

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

You cannot add software conference bridges to Cisco Unified Communications Manager by using Conference Bridge Configuration. Software conference bridges automatically get added when a Cisco Unified Communications Manager server gets added. After a Cisco Unified Communications Manager server gets added, the software conference bridge gets displayed in the Find/List Conference Bridges window (by default, the first software conference bridge gets configured during Cisco Unified Communications Manager installation) when you perform a search. You can update software conference bridges, but you cannot delete them.

See the Cisco Unified Communications Manager System Guide for more information about conference bridges.

The following table describes the software conference bridge configuration settings.

### Table 52: Software conference bridge configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Type</td>
<td>This field automatically displays Cisco Conference Bridge Software.</td>
</tr>
<tr>
<td>Host Server</td>
<td>This field automatically displays the Cisco Unified Communications Manager server for this software conference bridge.</td>
</tr>
<tr>
<td>Conference Bridge Name</td>
<td>This field automatically displays the software conference bridge name. The format of the name specifies CFB_ followed by a digit that represents the</td>
</tr>
<tr>
<td></td>
<td>value of the software conference bridge; for example, CFB_3 represents the third conference bridge in the Cisco Unified Communications Manager system.</td>
</tr>
<tr>
<td>Description</td>
<td>This field automatically displays a description, but the administrator can update this field.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool that has the highest priority within the Cisco Unified Communications Manager group that you are using or choose Default.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio</td>
</tr>
<tr>
<td></td>
<td>source, that support features and services for phone users.</td>
</tr>
<tr>
<td></td>
<td>Device configurations that are configured in the Common Device Configuration window display in the drop-down list.</td>
</tr>
</tbody>
</table>
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 conference bridge.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the System > Location menu option.

For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.

Use Trusted Relay Point

From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:

- Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
- Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.
- On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Cisco Unified CM 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 topics related to TRP insertion in Cisco Unified Communications Manager 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 CM 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 CM first tries to find a transcoder that is also designated as a TRP.

See topics related to trusted relay points and media resource management in the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.
Hardware Conference Bridge settings

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

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

**Note**

The hardware model type for Conference Bridge contains a specific Media Access Control (MAC) address and device pool information.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the hardware conference bridge configuration settings.

**Table 53: Hardware conference bridge configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Type</td>
<td>Choose Cisco Conference Bridge Hardware. For a description of this type, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB</td>
</tr>
<tr>
<td>Description</td>
<td>This field automatically generates from the MAC address that you provide. You can update this field if you choose.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool that has the highest priority within the Cisco Unified Communications Manager group that you are using or choose Default.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.</td>
</tr>
</tbody>
</table>
Uselocationstoimplementcalladmissioncontrol (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 conference bridge.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the System > Location menu option.

For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.

<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 conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the System &gt; Location menu option. For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>
| Use Trusted Relay Point  | From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:  
  - Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.  
  - Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  - On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 Cisco Unified Communications Manager System Guide for details of call behavior. If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM 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 CM first tries to find a transcoder that is also designated as a TRP. See the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points. |
| Special Load Information | Enter any special load information or leave blank to use default. |
Cisco IOS Conference Bridge settings

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

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support. See the Cisco Unified Communications Manager System Guide for more information about conference bridges.

The following table describes the Cisco IOS conference bridge configuration settings.

Table 54: Cisco IOS conference bridge configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Type</td>
<td>Choose Cisco IOS Conference Bridge or Cisco IOS Enhanced Conference Bridge.</td>
</tr>
<tr>
<td></td>
<td>For a description of these types, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Conference Bridge Name</td>
<td>Enter the same name that exists in the gateway Command Line Interface (CLI).</td>
</tr>
<tr>
<td></td>
<td>You can enter up to 15 characters. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-), and underscore (_).</td>
</tr>
<tr>
<td>Description</td>
<td>This field automatically generates from the conference bridge name that you provide. You can update this field if you choose.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool or choose Default.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users.</td>
</tr>
<tr>
<td></td>
<td>Device configurations that are configured in the Common Device Configuration window display in the drop-down list.</td>
</tr>
</tbody>
</table>
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 conference bridge.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the System > Location menu option.

For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.

<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 conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the System &gt; Location menu option. For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Device Security Mode</td>
<td>This field displays for Cisco IOS Enhanced Conference Bridge only. If you choose Non Secure Conference Bridge, the nonsecure conference establishes a TCP port connection to Cisco Unified Communications Manager on port 2000. <strong>Tip</strong> Ensure this setting matches the security setting on the conference bridge, or the call will fail. The Encrypted Conference Bridge setting supports the secure conference feature. See the Cisco Unified Communications Manager System Guide for secure conference bridge configuration procedures.</td>
</tr>
</tbody>
</table>
From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.
- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVP Agent).

If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior.

If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified CM first tries to find an RSVP Agent that can also be used as a TRP.

If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP.

See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

### Related Topics
- Location setup, on page 107
- Conference Bridge setup, on page 337
- Common device setup, on page 713

### Cisco Video Conference Bridge settings

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

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco video conference bridge configuration settings.
### Table 55: Cisco video conference bridge configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Type</td>
<td>Choose Cisco Video Conference Bridge (IPVC-35xx). For a description of this type, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB</td>
</tr>
<tr>
<td>Description</td>
<td>This field automatically generates from the conference bridge name that you provide. You can update this field if you choose.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool or choose Default.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.</td>
</tr>
<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 conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the <strong>System &gt; Location</strong> menu option. For an explanation of location-based CAC across intercluster trunks, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
</tbody>
</table>
From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.
- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVP Agent).

If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the Cisco Unified Communications Manager System Guide for details of call behavior.

If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified CM first tries to find an RSVP Agent that can also be used as a TRP.

If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP.

See the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.

### Product-Specific Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model-specific configuration fields that the device manufacturer defines</td>
<td>The device manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon under the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.</td>
</tr>
</tbody>
</table>

### Related Topics

- Location setup, on page 107
- Conference Bridge setup, on page 337
- Common device setup, on page 713
Cisco Conference Bridge (WS-SVC-CMM) settings

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

Be aware that both hardware and software conference bridges can be active at the same time. Software and hardware conference devices differ in the number of streams and the types of codec that they support.

See the Cisco Unified Communications Manager System Guide for more information about conference bridges. The following table describes the Cisco Conference Bridge (WS-SVC-CMM) configuration settings.

Table 56: Cisco conference bridge (WS-SVC-CMM) configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Type</td>
<td>Choose Cisco Conference Bridge (WS-SVC-CMM). For a description of this type, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description (up to 50 characters) or leave blank to generate automatically from the MAC address that you provide. Invalid characters comprise quotes (&quot;), angle brackets (&lt; &gt;), backslash (), ampersand (&amp;), and percent (%).</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter a unique device MAC address in this required field. MAC addresses comprise 12 hexadecimal digits (0-9, A-F). Example 1231123245AB</td>
</tr>
<tr>
<td>Subunit</td>
<td>From the drop-down list box, choose the value for the daughter card for a given slot on the Communication Media Module card.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool or choose Default.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.</td>
</tr>
</tbody>
</table>
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 conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the **System > Location** menu option.

For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong></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 conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the <strong>System &gt; Location</strong> menu option. For an explanation of location-based CAC across intercluster trunks, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
</tbody>
</table>
| **Use Trusted Relay Point**   | From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:  
  • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.  
  • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior.  
If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM 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 CM first tries to find a transcoder that is also designated as a TRP. See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points. |
| **Maximum Capacity**          | Choose the maximum number of streams for a given service on a daughter card. Possible values include 32, 64, 96, and 128 streams. Ensure that each daughter card has as many ports as the value that you choose. |
| **Product-Specific Configuration** |                                                                                                                                                                                                                 |
Cisco IOS Heterogeneous Video Conference Bridge settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Heterogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports heterogeneous video conferences. In a heterogeneous video conference, all the conference participants connect to the conference bridge with phones that use different video format attributes. In heterogeneous conferences, transcoding and transsizing features are required from the DSP to convert the signal between the various formats.

For heterogeneous video conferences, callers connect to the conference as audio participants under either of the following conditions:

- Insufficient DSP resources.
- The conference bridge is not configured to support the video capabilities of the phone.

See the Cisco Unified Communications Manager System Guide for more information about conference bridges. The following table describes the Cisco IOS Heterogeneous Video Conference Bridge configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Name</td>
<td>Enter a name for your conference bridge.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for your conference bridge.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool or choose Default.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Common Device Configuration | Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users.  
Device configurations that are configured in the Common Device Configuration window display in the drop-down list. |
| Location                  | Use location 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 conference bridge.  
A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.  
To configure a new location, use the System > Location menu option.  
For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide. |
| Use Trusted Relay Point    | From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint.  
• Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.  
• Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
• On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.  
Cisco Unified CM 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 Cisco Unified Communications Manager System Guide for details of call behavior.  
If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified CM first tries to find an RSVP Agent that can also be used as a TRP.  
If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP.  
See the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points. |
Cisco IOS Guaranteed Audio Video Conference Bridge settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me voice and video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Guaranteed Audio Video Conference Bridge specifies the IOS-based video conference bridge type where DSP resources are reserved for the audio portion of the conference, and video service is not guaranteed. Callers on video phones may have video service if DSP resources are available at the start of the conference. Otherwise, the callers connect to the conference as audio participants.

See the Cisco Unified Communications Manager System Guide for more information about conference bridges.

The following table describes the Cisco IOS Heterogeneous Video Conference Bridge configuration settings.

**Table 58: Cisco IOS guaranteed audio video conference bridge settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Name</td>
<td>Enter a name for your conference bridge</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for your conference bridge</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool or choose Default.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.</td>
</tr>
</tbody>
</table>
Use location 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 conference bridge.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the System > Location menu option.

For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Use location 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 conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the System &gt; Location menu option. For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Use Trusted Relay Point</td>
<td>From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>• Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>• On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified CM 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).</td>
</tr>
<tr>
<td></td>
<td>If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the Cisco Unified Communications Manager System Guide for details of call behavior.</td>
</tr>
<tr>
<td></td>
<td>If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP.</td>
</tr>
<tr>
<td></td>
<td>If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP.</td>
</tr>
<tr>
<td></td>
<td>See the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.</td>
</tr>
</tbody>
</table>

Related Topics
Location setup, on page 107
Conference Bridge setup, on page 337
Cisco IOS Homogeneous Video Conference Bridge settings

Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Cisco IOS Homogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports homogeneous video conferences. A homogeneous video conference is a video conference in which all participants connect using the same video format attributes. All the video phones support the same video format and the conference bridge sends the same data stream format to all the video participants.

If the conference bridge is not configured to support the video format of a phone, the caller on that phone connects to the conference as an audio only participant.

See the Cisco Unified Communications Manager System Guide for more information about conference bridges.

The following table describes the Cisco IOS Homogeneous Video Conference Bridge configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Name</td>
<td>Enter a name for your conference bridge.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for your conference bridge</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool or choose Default.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users.</td>
</tr>
<tr>
<td></td>
<td>Device configurations that are configured in the Common Device Configuration window display in the drop-down list.</td>
</tr>
<tr>
<td>Location</td>
<td>Use location 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.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, choose the appropriate location for this conference bridge.</td>
</tr>
<tr>
<td></td>
<td>A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.</td>
</tr>
<tr>
<td></td>
<td>To configure a new location, use the System &gt; Location menu option.</td>
</tr>
<tr>
<td></td>
<td>For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>
From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint.

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.

- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior.

If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM 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 CM first tries to find a transcoder that is also designated as a TRP.

See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

### Related Topics

- Location setup, on page 107
- Conference Bridge setup, on page 337
- Common device setup, on page 713

### Cisco TelePresence MCU settings

Cisco TelePresence MCU refers to a set of hardware conference bridges for Cisco Unified Communications Manager.

The Cisco TelePresence MCU is a high-definition (HD) multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full trans-coding, and is ideal for mixed HD endpoint environments.

The Cisco TelePresence MCU supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control and monitoring of the system and conferences. The Cisco TelePresence MCU provides XML management API over HTTP.

Cisco TelePresence MCU allows both ad hoc and meet-me voice and video conferencing. Each conference bridge can host several simultaneous, multiparty conferences.
See the *Cisco Unified Communications Manager System Guide* for more information about conference bridges.

The following table describes the Cisco TelePresence MCU configuration settings.

**Table 60: Cisco TelePresence MCU configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Bridge Name</td>
<td>Enter a name for your conference bridge</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Enter the IP Address of the Cisco TelePresence MCU conference bridge</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for your conference bridge</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool or choose Default.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to assign to the conference bridge. The common device configuration includes attributes, such as MOH audio source, that support features and services for phone users. Device configurations that are configured in the Common Device Configuration window display in the drop-down list.</td>
</tr>
<tr>
<td>Location</td>
<td>Use location 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 conference bridge. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this conference bridge consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the <strong>System &gt; Location</strong> menu option. For an explanation of location-based CAC across intercluster trunks, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Trusted Relay Point</td>
<td>From the drop-down list box, enable or disable whether Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>• Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>• On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>A TRP device designates an MTP or transcoder device that is labeled as Trusted Relay Point.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified CM 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).</td>
</tr>
<tr>
<td></td>
<td>If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the <em>Cisco Unified Communications Manager System Guide</em> for details of call behavior.</td>
</tr>
<tr>
<td></td>
<td>If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM first tries to find an RSVPAgent that can also be used as a TRP.</td>
</tr>
<tr>
<td></td>
<td>If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP.</td>
</tr>
<tr>
<td></td>
<td>See the <em>Cisco Unified Communications Manager System Guide</em> for a complete discussion of network virtualization and trusted relay points.</td>
</tr>
<tr>
<td>SIP Interface Info</td>
<td></td>
</tr>
<tr>
<td>MCU Conference Bridge SIP Port</td>
<td>This is the SIP listening port of the Cisco TelePresence MCU Conference Bridge. The default value is 5060.</td>
</tr>
<tr>
<td>SIP Profile</td>
<td>From the drop-down list box, choose <strong>Standard SIP Profile for TelePresence Conferencing</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP Trunk Security Profile</td>
<td>From the drop-down list box, choose the security profile to apply to the SIP trunk. You must apply a security profile to all SIP trunks. Cisco Unified Communications Manager provides a default nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile. To identify the settings that each profile contains, choose System &gt; Security Profile &gt; SIP Trunk Security Profile. If you are using SRTP with Cisco TelePresence MCU, the SIP trunk security profile must use the following settings: • Device Security Mode must be Encrypted • Incoming Transport Type and Outgoing Transport Type must be TLS • X.509 Subject Name must be set to the defined Common Name that is used in the Cisco TelePresence MCU certificates For information on how to configure security profiles, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
| SRTP Allowed          | Check the SRTP Allowed check box if you want Cisco Unified Communications Manager to allow secure and nonsecure calls with Cisco TelePresence MCU. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the Cisco TelePresence MCU and uses RTP instead. For more information on encryption, see the Cisco Unified Communications Manager Security Guide.  
**Note** When this check box is checked, the vcs-interop script is selected by default in the Script drop-down list box and the Enable Trace check box is checked.  
**Note** If you check this check box, you must configure TLS so that you do not expose keys and other security-related information during call negotiations. |
| Normalization Script info |                                                                                                                                                                                                                           |
| Script                | Choose the script from the drop-down list box that you want to apply. To import another script for Cisco TelePresence MCU, go to the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script), and import a new script file. |
| Enable Trace          | Check this check box to enable tracing within the script or uncheck this check box to disable tracing. When this box is checked, the trace.output API that is provided to the Lua scripter produces an SDI trace.  
**Note** Cisco recommends that you enable tracing only while debugging a script. Tracing has an impact on performance and should not be enabled under normal operating conditions. |
### Field Description

| Parameter Name/Parameter Value | (Optional) Enter parameter names and parameter values. Valid values include all characters except equal signs (=), semicolons (;), and nonprintable characters, such as tabs. You can enter a parameter name with no value.  
Example  
Parameter Name Parameter Value  
CCA-ID 11223344  
pbx  
location RTP  
You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values.  
To add another parameter line, click the + (Plus) button. To delete a parameter line, click the – (Minus) button. |

### HTTP Interface Info

| Username | Enter the Cisco TelePresence MCU administrator username. |
| Password | Enter the Cisco TelePresence MCU administrator password. |
| Confirm Password | Enter the Cisco TelePresence MCU administrator password. |
| Use HTTPS | Check this check box if you want to create a secure HTTPS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU. The default HTTPS port is 443.  
For information on how to create a TLS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU, see topics related to setting up a TLS connection with Cisco TelePresence MCU. |
| HTTP Port | Enter the Cisco TelePresence MCU HTTP port. The default port is 80. |

**Note**  
The HTTP configuration must match what is configured on the Cisco TelePresence MCU. This information allows Cisco Unified Communications Manager to invoke the remote management API on the Cisco TelePresence MCU.

**Related Topics**
- Location setup, on page 107  
- Conference Bridge setup, on page 337  
- Common device setup, on page 713

**CSCub65671 Route Class Configuration SIP Information**

If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class.
You can 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.

Set up TLS connection with Cisco TelePresence MCU

If you are using SRTP with Cisco TelePresence MCU, you must set up a TLS connection with Cisco TelePresence MCU so that you do not expose keys and other security-related information during call negotiations.

Note

This procedure details tasks that are performed in Cisco Unified Communications Manager. For detailed instructions on how to import and export certificates in Cisco TelePresence MCU, see your Cisco TelePresence MCU product documentation.

Procedure

Step 1 Download the Cisco Unified Communications Manager security certificate by performing the following steps:
   a) In Cisco Unified Operating System Administration, choose **Security > Certificate Management**.
   b) Click **Find**.
   c) Click **CallManager.pem** to view the certificate.
   d) Click **Download** and save the file to a local drive.

Step 2 Upload the Cisco Unified Communications Manager certificate to Cisco TelePresence MCU.

Step 3 Generate self-signed certificates for Cisco TelePresence MCU and save the certificates to a local drive.

Step 4 Upload self-signed certificates to the Cisco TelePresence MCU.

Step 5 Upload Cisco TelePresence MCU certificates to Cisco Unified Communications Manager by doing the following:
   a) In Cisco Unified Operating System Administration, choose **Security > Certificate Management**.
   b) Click **Upload Certificate/Certificate Chain**.
   c) From the Certificate Name drop-down list box, choose **CallManager-trust**.
   d) Click **Browse** and locate the Cisco TelePresence MCU certificate that you saved locally.
   e) Click **Upload File** to upload certificates.

Step 6 In Cisco Unified Communications Manager Administration, choose **System > Security > SIP Trunk Security Profile** and create a secure SIP Trunk Security Profile that uses the following settings:
   - Device Security Mode must be Encrypted
   - Incoming Transport Type and Outgoing Transport Type must be TLS
   - X.509 Subject Name must be set to the defined Common Name that is used in the Cisco TelePresence MCU certificates

Step 7 On the Cisco TelePresence MCU, configure SIP signaling encryption with TLS, and media encryption with SRTP.
Synchronize conference device settings

To synchronize a conference device with the most recent configuration changes, perform the following procedure, which applies 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 Media Resources > Conference Bridge. The Find and List Conference Bridges window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find. The window displays a list of conference bridges that match the search criteria.

Step 4 Check the check boxes next to the conference bridges that you want to synchronize. To choose all conference bridges in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected. The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

Conference Bridge setup, on page 337
Synchronize conference device settings
Media termination point setup

This chapter provides information to add, update, and delete media termination points. For additional information, see topics related to the following in the Cisco Unified Communications Manager System Guide:

- Transcoders
- Media Termination Points
- Resource Reservation Protocol
- Media Resource Management
- About media termination point setup, page 363
- Cisco IOS media termination point setup, page 364
- Cisco IOS media termination point deletion, page 364
- Cisco IOS media termination point settings, page 365
- Synchronize media termination point, page 365

About media termination point setup

A Media Termination Point software device allows Cisco Unified Communications Manager to relay calls that are routed through SIP or H.323 endpoints or gateways. You can allocate a media termination point device because of DTMF or RSVP requirements. When a media termination point is allocated for RSVP, you can insert it between any type of endpoint device, including SIP or H.323 devices.

Media termination point, a Cisco software application, installs on a server during the software installation process. You must activate and start the Cisco IP Voice Media Streaming Application service on the server on which you configure the media termination point device. For information on activating and starting services, see the Cisco Unified Serviceability Administration Guide.

Each media termination point device that is defined in the database registers with the Media Resource Manager (MRM). The MRM keeps track of the total available media termination point devices in the system and of which devices have available resources.
During resource reservation, the MRM determines the number of resources and identifies the media resource type (in this case, the media termination point) and the location of the registered media termination point device. The MRM updates its share resource table with the registration information and propagates the registered information to the other Cisco Unified Communications Managers within the cluster.

The media termination point and transcoder can register with the same Cisco Unified Communications Manager.

Each media termination point receives a list of Cisco Unified Communications Managers, in priority order, to which it should attempt to register. Each media termination point can register with only one Cisco Unified Communications Manager at a time.

Depending on the capabilities of the SIP endpoint, Cisco Unified Communications Manager may require an RFC 2833 DTMF-compliant media termination point device to make SIP calls. For RSVP calls, the Media Resource Group List (MRGL) that is associated with the endpoint device needs to include the media termination point devices that support RSVP.

### Related Topics

Transcoder setup, on page 367

### Cisco IOS media termination point setup

In Cisco Unified Communications Manager Administration, use the **Media Resources > Media Termination Point** menu path to configure media termination points (MTPs).

**Media termination point configuration tips**

Make sure that the following prerequisites are met before you proceed with configuration of a media termination point:

- Ensure servers are configured.
- Ensure device pools are configured.

You can have only one Media Termination Point device for each Cisco Unified Communications Manager server. When a Cisco Unified Communications Manager Server is added, a media termination point device automatically gets created for the server but is not available for use until the Cisco IP Voice Media Streaming App service gets activated.

### Cisco IOS media termination point deletion

Before deleting a media termination point that is currently in use and is the last device in the Media Resource Group, you should perform either or both of the following tasks:

- Assign a different media termination point to the media resource groups that are using the media termination point that you want to delete.
- Delete the media resource groups that are using the media termination point that you want to delete.

**Related Topics**

- About media resource group setup, on page 371
- Media resource group deletion, on page 372

## Cisco IOS media termination point settings

The following table describes Cisco IOS media termination point settings.

### Table 61: Cisco IOS media termination point settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Termination Point Type</td>
<td>Choose Cisco IOS Enhanced Software Media Termination Point. For specific information on this media termination point type, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>Media Termination Point Name</td>
<td>Enter a name for the media termination point, up to 15 alphanumeric characters. <strong>Note</strong>: You cannot use special characters as the MTP name; for example !, @, #, $, or %. <strong>Tip</strong>: Ensure that you enter the same media termination point name that exists in the gateway Command Line Interface (CLI).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter any description for the media termination point.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose a device pool that has the highest priority within the Cisco Unified Communications Manager group that you are using or choose Default.</td>
</tr>
<tr>
<td>Trusted Relay Point</td>
<td>Check this check box to designate this media termination point (MTP) as a trusted relay point (TRP) that Cisco Unified Communications Manager can use in a network virtualization environment. **See the <em>Cisco Unified Communications Manager System Guide</em> for a discussion of trusted relay points.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Media termination point setup, on page 363

## Synchronize media termination point

To synchronize a Media Termination Point with the most recent configuration changes, perform the following procedure, which applies 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 **Media Resources > Media Termination Point**.
The Find and List a Media Termination Points window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find.
The window displays a list of a Media Termination Points that match the search criteria.

**Step 4** Check the check boxes next to the Media Termination Points that you want to synchronize. To choose all Media Termination Points in the window, check the check box in the matching records title bar.

**Step 5** Click **Apply Config to Selected**.
The Apply Configuration Information dialog displays.

**Step 6** Click OK.

Related Topics

- Media termination point setup, on page 363
Transcoder setup

This chapter provides information to configure transcoders. For additional information, see topics related to transcoders and media resource management in the Cisco Unified Communications Manager System Guide.

- About transcoder setup, page 367
- Transcoder deletion, page 367
- Transcoder settings, page 368
- Synchronize transcoder, page 369

About transcoder setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Transcoder menu path to configure transcoders.

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

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

A transcoder control process gets created for each transcoder device that is defined in the database. Each transcoder registers with the MRM when it initializes. The MRM keeps track of the transcoder resources and advertises their availability throughout the cluster.

Transcoder deletion

You cannot delete a transcoder that is assigned to a media resource group. To find out which media resource groups are using the transcoder, from the Transcoder Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the
system, the dependency records summary window displays a message. If you try to delete a transcoder that is in use, Cisco Unified Communications Manager displays a message. Before deleting a transcoder that is currently in use, you must remove the transcoder from the media resource group(s) to which it is assigned.

Related Topics
Access dependency records, on page 874

Transcoder settings

The following table describes the transcoder settings.

Table 62: Transcoder settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transcoder Type</td>
<td>Choose the appropriate transcoder type: Cisco Media Termination Point Hardware, Cisco IOS Media Termination Point, Cisco IOS Enhanced Media Termination Point, or Cisco Media Termination Point (WS-SVC-CMM). For specific information on these transcoder types, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description (up to 128 characters) or leave blank to generate automatically from the MAC address or device name that you provide.</td>
</tr>
<tr>
<td>Device Name</td>
<td>This field displays if you chose Cisco IOS Media Termination Point or Cisco IOS Enhanced Media Termination Point as the transcoder type. Enter the same transcoding name that you entered in the gateway Command Line Interface (CLI). Enter up to 15 characters. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), as well as dot (.), dash (-), and underscore (_).</td>
</tr>
<tr>
<td>Transcoder Name</td>
<td>For Cisco Media Termination Point (WS-SVC-CMM) transcoders, the system fills in this value based on the MAC address that you provide.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>For Cisco media termination point hardware or Cisco Media Termination Point (WS-SVC-CMM), enter a MAC address, which must be 12 characters.</td>
</tr>
<tr>
<td>Subunit</td>
<td>For Cisco Media Termination Point (WS-SVC-CMM) transcoders, choose a subunit from the drop-down list box.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>From the drop-down list box, choose a device pool. For more detailed information on the chosen device pool, click View Details.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>From the drop-down list box, choose a common device configuration. For more detailed information on the chosen common device configuration, click View Details.</td>
</tr>
</tbody>
</table>
Enter any special load information into the Special Load Information field or leave blank to use default. Valid characters include letters, numbers, dashes, dots (periods), and underscores.

Check this check box to designate this transcoder as a trusted relay point (TRP) that Cisco Unified Communications Manager can use in a network virtualization environment.

See the *Cisco Unified Communications Manager System Guide* for a discussion of trusted relay points.

For Cisco Media Termination Point (WS-SVC-CMM) transcoders, choose a maximum capacity from the drop-down list box.

The device manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice.

To view field descriptions and help for product-specific configuration items, click the “?” information icon below the Product Specific Configuration heading to display help in a popup dialog box.

If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.

**Related Topics**

Transcoder setup, on page 367

**Synchronize transcoder**

To synchronize a transcoder with the most recent configuration changes, perform the following procedure, which applies 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 Media Resources > Transcoder.
The Find and List Transcoders window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find.
The window displays a list of transcoders that match the search criteria.
Step 4 Check the check boxes next to the transcoders that you want to synchronize. To choose all transcoders in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected. The Apply Configuration Information dialog displays.

Step 6 Click OK.

Related Topics

Transcoder setup, on page 367
Media resource group setup

This chapter provides information to configure media resource groups. You can group devices of the following types into a single media resource group:

- Conference Bridge (CFB)
- Media Termination Point (MTP)
- Music On Hold Server (MOH)
- Transcoder (XCODE)
- Annunciator (ANN)

For additional information, see topics related to media resources, media resource groups, and media resource group lists in the Cisco Unified Communications Manager System Guide.

- About media resource group setup, page 371
- Media resource group deletion, page 372
- Media resource group settings, page 372

About media resource group setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Media Resource Group menu path to configure media resource groups.

Media resource management comprises working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources, so all Cisco Unified Communications Managers within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and music on hold services.

You can associate a media resource group, a logical grouping of media servers, with a geographical location or with a site as desired. You can also form media resource groups to control the usage of servers or the type of service (unicast or multicast) that is desired.
**Media resource group configuration tips**

Be aware that you cannot delete a media resource, such as a conference bridge, that is part of a media resource group unless you first remove the resource from the media resource group or you delete the media resource group that contains the media resource.

**Media resource group deletion**

You cannot delete a media resource group that is assigned to a Media Resource Group List. To find out which media resource groups lists are using the media resource group, in the Media Resource Group Configuration window, from the Related Links drop-down list box, choose Dependency Records and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a media resource group that is in use, Cisco Unified Communications Manager displays a message. Before deleting a media resource group that is currently in use, you must perform either or both of the following tasks:

- Assign a different media resource group list to any media resource groups that are using the media resource group that you want to delete.
- Delete the media resource group lists that are using the media resource group that you want to delete.

**Related Topics**

- About media resource group list setup, on page 375
- Media resource group list deletion, on page 375
- Access dependency records, on page 874

**Media resource group settings**

The following table describes the settings that are used for configuring media resource groups.

*Table 63: Media resource group settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name in this required field for the Cisco Unified Communications Manager to identify the media resource group. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the media resource group. 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>
<tr>
<td>Devices for this Group</td>
<td>This area comprises two panes that are used to define the media resources for a media resource group: Available Media Resources and Selected Media Resources.</td>
</tr>
</tbody>
</table>
### Field Description

**Available Media Resources**

This pane lists the media resources that can be chosen for a media resource group. The list includes the following media resource types:

- Conference Bridges (CFB)
- Media Termination Points (MTP)
- Music On Hold Servers (MOH)
- Transcoders (XCODE)
- Annunciator (ANN)

Music on hold servers that are configured for multicast get labeled as (MOH)[Multicast].

To add a media resource for this media resource group, choose one from the list and click the down arrow. After a media resource is added, its name moves to the Selected Media Resources pane.

**Selected Media Resources**

This pane lists the media resources that were chosen for a media resource group. For any media resource group, you must choose at least one media resource.

To delete (unselect) a media resource, choose its name in the list and click the up arrow.

**Use Multicast for MOH Audio (If at least one multicast MOH resource is available)**

To use multicast for Music On Hold Audio, check this check box. To do so, make sure that at least one of the selected media resources is a multicast MOH server.

**Note**
The system administrator configures or creates multicast audio sources.

### Related Topics

- Media resource group setup, on page 371
Media resource group settings
Media resource group list setup

This chapter provides information to configure Media Resource Group Lists. For additional information, see topics related to media resources, media resource groups, and media resource group lists in the *Cisco Unified Communications Manager System Guide*.

- About media resource group list setup, page 375
- Media resource group list deletion, page 375
- Media resource group list settings, page 376

**About media resource group list setup**

In Cisco Unified Communications Manager Administration, use the Media Resources > Media Resource Group List menu path to configure media resource group lists.

Media resource management comprises working with media resource groups and media resource group lists. Media resource management provides a mechanism for managing media resources, so all Cisco Unified Communications Managers within a cluster can share them. Media resources provide conferencing, transcoding, media termination, annunciator, and music on hold services.

A Media Resource Group List provides a prioritized grouping of media resource groups. An application selects the required media resource, such as a music on hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.

**Media resource group list configuration tips**

Be aware that you cannot delete a media resource group that is assigned to a Media Resource Group List unless you first remove the media resource group from the Media Resource Group List(s) to which it is assigned or you delete the Media Resource Group List.

**Media resource group list deletion**

Be aware that you cannot delete a Media Resource Group List that is assigned to a device pool(s) or to a device(s). You must first modify the device pool(s) or device(s) to which a Media Resource Group List is assigned.
Media resource group list settings

The following table describes the settings that are used for configuring Media Resource Group Lists.

### Table 64: Media resource group list settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Resource Group List Information</td>
<td>Enter a unique name in this required field for the Cisco Unified Communications Manager to identify the Media Resource Group List. This name can comprise up to 50 characters. Valid characters include letters, numbers, spaces, dashes, dots (periods), and underscores.</td>
</tr>
<tr>
<td>Name</td>
<td>This window lists the media resource groups that can be chosen for a Media Resource Group List. The list includes only previously defined media resource groups. To add a media resource group for this Media Resource Group List, choose one from the list and click the down arrow that is located between the two panes. After a media resource group is added, its name moves to the Selected Media Resource Groups pane.</td>
</tr>
<tr>
<td>Available Media Resource Groups</td>
<td>This pane lists the media resource groups that were chosen for a Media Resource Group List. For any Media Resource Group List, you must choose at least one media resource group. To delete (unselect) a media resource group, choose its name in the list and click the up arrow that is located between the two panes. Because media resource groups are listed in order of priority (highest to lowest), you must use the up and down arrows that are located to the right of this pane to reorder the media resource group priority. To do so, choose a media resource group in the list and use the up or down arrow to change its priority.</td>
</tr>
<tr>
<td>Selected Media Resource Groups</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Media resource group list setup, on page 375
Announcement setup

The chapter provides information about using Cisco-provided announcements and tones. For additional information, see topics related to External Call Control in the Cisco Unified Communications Manager Features and Services Guide.

- Cisco-provided announcements and tones, page 377
- About announcement setup, page 378
- Announcement deletions, page 379
- Announcement settings, page 379
- Announcements in the Find and List Announcements Window, page 380
- Upload customized announcement, page 381
- Play announcement, page 382

Cisco-provided announcements and tones

Cisco-provided announcements and tones are installed automatically when you install Cisco Unified Communications Manager. These announcements and tones are displayed in the Find and Lists Announcements window in Cisco Unified Communications Manager Administration. Announcements can be used for:

- Basic calls
- External call control
- Multilevel Precedence and Preemption (MLPP)

Selecting Media Resources > Announcements in Cisco Unified Communications Manager allows you to use the existing Cisco-provided announcements, insert custom announcement .wav files, assign the locale for the announcement, change the description for the announcement, or change the message or tone that you wish an announcement to play.

Related Topics
- Announcement setup, on page 377
About announcement setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Announcements menu path to configure announcements.

There are two classifications of announcements:

- System Announcements
- Feature Announcements

System announcements are pre-defined announcements that are used in normal call processing or provided as sample feature announcements. Feature announcements are used by specific features such as Music On Hold (MoH) in association with Hunt Pilot call queuing or External Call Control.

There are up to 50 feature announcements available using the Add New button. These announcements may be Cisco-provided audio files or uploaded custom wav files. All custom announcement wav files must be uploaded to all servers in the cluster.

**Note**

Announcements are specific to the locale (language). If your installation is using more than one language locale, each custom announcement must be recorded in each language as a separate wav file and uploaded with the correct locale assignment. This also requires that the correct locale package be installed on each server before uploading custom announcement wav files for languages other than United States English.

From the Announcement Listing window, clicking on the announcement identifier for an announcement produces an announcement configuration dialog. Within this dialog you can edit the announcement description and other settings. If one or more custom wav files have been uploaded for the announcement, a list of the custom wav files for each locale (language) is created. Each of these files also have an Enable check-box to indicate if the custom wav file should be used. If the check-box is unchecked, then the selected Cisco audio file is used.

Like MoH audio source files, the recommended format for announcements includes the following specifications:

- 16-bit PCM wav file
- Stereo or mono
- Sample rates of 48 kHz, 44.1 kHz, 32 kHz, 16 kHz, or 8 kHz

**Tip**

When a call is routed to a queue-enabled Hunt Pilot that is configured with MoH, and has an initial announcement configured (with "Play Always" and early media cut through), the greeting is played to the caller before the called party is alerted about the call. Trunks and gateways must also support early media cut through for the greeting to be played. Cisco PRI/MGCP gateways, H.323 gateways and trunks support early media cut through. For SIP trunk to support early media cut through, you must enable PRACK. Be aware that a greeting may not be played if the device does not support early media cut through.
# Announcement deletions

You cannot delete any System or Feature announcements that are configured for use within Cisco Unified Communications Manager Administration (such as MoH). In these instances, a selection check-box will not appear. To delete a feature announcement, select the check-box and click on the **Delete** button.

# Announcement settings

The following table describes the announcement settings.

*Table 65: Announcement settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Announcement Configuration and Upload File Windows</td>
<td></td>
</tr>
<tr>
<td>Announcement Identifier</td>
<td>The Announcement Identifier is a text box to assign a meaningful identifying name to the announcement. This field cannot be modified for System Announcements. This field must be unique (different from all other announcements). The Announcement Identifier is used when selecting an announcement for a feature such as Music-on-Hold.</td>
</tr>
<tr>
<td>Customized Description</td>
<td>For customized announcements that you are inserting, enter a description for the announcement; for example, enter the text from the customized announcement. You can enter any characters in this field. When you click the Upload File button in the Find and List window, this field displays as blank. When you click the Upload File button in the Announcements Configuration window, the Cisco-provided (default) description for the announcement displays. If you do not update this field in the Announcements Configuration window, the Cisco-provided (default) description displays. After you update this customized description field, the Cisco-provided default description displays in the Find and Lists Announcements window; see the Default Description column in the Find and Lists window for the default description. You can enter up to 50 characters.</td>
</tr>
<tr>
<td>Locale</td>
<td>This setting displays in the Upload File window. From the Locale drop-down list box, choose the locale that you want to associate with the announcement. By default, all Cisco-provided announcements support English United States. If a Cisco Unified Communications Locale has been installed, the Cisco-provided announcements are provided for that locale in addition to other installed locales. For a locale to display in the Locale drop-down list box in the Upload File Configuration window, you must install the Cisco Unified Communications Locale Installer that is specific to your locale(s). For more information, see the <em>Cisco Unified Communications Operating System Administration Guide</em>.</td>
</tr>
</tbody>
</table>
From the drop-down list box, choose the Cisco-provided announcement that you want to play when the custom announcement is not used. If <None> is selected from the list box, no Cisco-provided announcement will be used.

This section only appears if a custom announcement .wav file has been uploaded for the announcement.

This setting displays after you insert a customized announcement. When the Enable check box is checked, Cisco Unified Communications Manager plays the customized announcement for the locale that is shown. If you want Cisco Unified Communications Manager to play the Cisco-provided announcement that is associated with the announcement identifier, uncheck the Enable check box.

This field, which is read-only, displays the description for the customized announcement for the displayed locale. You enter this description when you upload the customized announcement.

This field, which is read-only, displays the locale that you chose for the customized announcement when you uploaded the .wav file. Each locale is associated with an uploaded custom announcement. You can upload another wav file for the same announcement, but you assign it to a different locale. In this case, two rows display, one for each locale. If you want to update or replace a custom announcement for a locale, you can upload a new wav file with the same locale you want to replace.

This field indicates the last uploaded customized announcement file name.

You can upload custom announcement wav files or change the Cisco-provided file for a System announcement, however; you cannot change the announcement identifier. For example, the System announcement (VCA_00121) is played when a caller dials an invalid number. This is commonly known as the "vacant call announcement" and could be modified with an uploaded custom wav file with a different announcement.

You cannot update announcements that are not hyperlinked in the Find and List Announcements window. You can insert customized announcements for Cisco-provided announcements that are underlined with a hyperlink in the Find and List Announcements window; for example, Custom_5001, Custom_5014, MLPP-ICA_00120, or MonitoringWarning_00055. For more information on how to upload a customized announcement, see the following sections:
The following table describes the announcements that display in the Find and List Announcements window. This list is an initial example and may change based on feature announcements being inserted and future upgrades.

**Table 66: Announcements in the Find and List Announcements window**

<table>
<thead>
<tr>
<th>Announcement Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP-BNEA_00123</td>
<td>System: MLPP Busy not equipped</td>
</tr>
<tr>
<td>MLPP-BPA_00122</td>
<td>System: MLPP Higher precedence</td>
</tr>
<tr>
<td>MLPP-ICA_00120</td>
<td>System: MLPP Service disruption</td>
</tr>
<tr>
<td>MLPP-PALA_00119</td>
<td>System: MLPP Precedence access limit</td>
</tr>
<tr>
<td>MLPP-UPA_00124</td>
<td>System: MLPP Unauthorized precedence</td>
</tr>
<tr>
<td>Mobility_VMA</td>
<td>Please press 1 to be connected</td>
</tr>
<tr>
<td>MonitoringWarning_00055</td>
<td>System: Monitoring or Recording</td>
</tr>
<tr>
<td>RecordingWarning_00038</td>
<td>System: Recording</td>
</tr>
<tr>
<td>VCA_00121</td>
<td>System: Vacant number / invalid number dialed</td>
</tr>
<tr>
<td>Wait_In_Queue_Sample</td>
<td>Builtin: Sample queued caller periodic announcement</td>
</tr>
<tr>
<td>Welcome_Greeting_Sample</td>
<td>Builtin: Sample caller greeting</td>
</tr>
</tbody>
</table>

**Upload customized announcement**

Perform the following procedure to upload a customized announcement.

**Procedure**

**Step 1** In Cisco Unified Communications Manager Administration, choose Media Resources > Announcements. The Find and List Announcements window displays.

**Step 2** In the Find and List Announcements window, click the hyperlink for the announcement (for example, Wait In Queue Sample). When the Announcements window displays, click Upload File.

**Step 3** In the Upload File pop-up window, choose the locale, enter the filename or browse to select the .wav file and click Upload File.
The upload process begins, and may take a few minutes depending on the file. The Status is updated once processing is complete. Select Close to close the upload window.

**Step 4** The Announcement Configuration window refreshes to update the uploaded file status.

**Step 5** If you want Cisco Unified Communications Manager to play the customized announcement instead of playing the Cisco-provided announcement, make sure that the Enable check box displays as checked in the Announcement by Locale pane in the Announcements Configuration window. If the Enable check box is unchecked, Cisco Unified Communications Manager plays the Cisco-provided announcement.

**Step 6** Once the changes have been made in the Announcements Configuration window, click Save.

---

**What to Do Next**

You must upload the announcement on each node in the cluster as the announcement files are not propagated between servers in a cluster. Browse Cisco Unified Communications Manager Administration on each server in the cluster and repeat the upload process.

**Related Topics**

- Announcement setup, on page 377
- About announcement setup, on page 378

---

**Play announcement**

After you insert the custom announcement, Cisco Unified Communications Manager automatically plays the custom announcement, unless you uncheck the Enable check box in the Announcements by Locale pane in the Announcements Configuration window (which indicates that you want Cisco Unified Communications Manager to play the Cisco-provided announcement that is associated with the announcement identifier).
Other media resource menu options

This chapter provides brief descriptions of selected Media Resource menu options. A pointer to the documentation where more detailed information is available for the option is provided.

- Music On Hold audio source setup, page 383
- Fixed MOH audio source setup, page 383
- Music On Hold server setup, page 384
- MOH audio file management setup, page 384
- Mobile voice access setup, page 384

Music On Hold audio source setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Music On Hold Audio Source menu path to configure Music On Hold audio sources.

The integrated Music On Hold feature provides the ability to place on-net and off-net users on hold with music that is 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

Music on hold configuration comprises configuration of music on hold audio sources and music on hold servers.

For more information on how to use the Music On Hold Audio Source Configuration window, see the Cisco Unified Communications Manager Features and Services Guide.

Fixed MOH audio source setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Fixed MOH Audio Source menu path to configure the fixed Music On Hold audio source.

The integrated Music On Hold feature provides the ability to place on-net and off-net users on hold with music that is streamed from a streaming source. This feature includes the following actions:
Music on hold configuration comprises configuration of music on hold audio sources and music on hold servers. You can also enable a music on hold fixed audio source, and this audio source can allow multicasting.

For more information on how to use the Fixed MOH Audio Source Configuration window, see the Cisco Unified Communications Manager Features and Services Guide.

Music On Hold server setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Music On Hold Server menu path to configure fixed Music On Hold servers.

The Cisco Unified Communications Manager Music On Hold feature uses the 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.

For more information on how to use the Music On Hold Server Configuration window, see the Cisco Unified Communications Manager Features and Services Guide.

MOH audio file management setup

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.

For more information on how to use the MOH Audio File Management Configuration window, see the Cisco Unified Communications Manager Features and Services Guide.

Mobile voice access setup

In Cisco Unified Communications Manager Administration, use the Media Resources > Mobile Voice Access menu path to configure sets of localized user prompts for Mobile Voice Access.

Mobile Connect allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Mobile Voice Access is the associated integrated voice response (IVR) system, which allows users to turn Mobile Connect on or off and to initiate calls from a cellular phone or other remote phone as if the call were initiated from the desktop phone.

The Mobile Voice Access window contains settings for localized user IVR prompts. For more information on how to configure Mobile Connect and Mobile Voice Access, see the Cisco Unified Communications Manager Features and Services Guide.
PART V

Advanced features setup

- Cisco voice-mail port setup, page 387
- Cisco Voice Mail Port Wizard, page 395
- Message waiting setup, page 403
- Cisco voice-mail pilot setup, page 407
- Voice-mail profile setup, page 411
- Other advanced features menu options, page 415
Cisco voice-mail port setup

This chapter provides information to add and delete Cisco voice-mail ports in the Cisco Unified Communications Manager database without using the Cisco Voice Mail Port Wizard.

For additional information, see the Cisco Unity and Cisco Unity Connection Configuration Checklist, Cisco Unified Communications Manager System Guide.

- About Cisco voice-mail port setup, page 387
- Cisco voice-mail port deletion, page 388
- Cisco voice-mail port settings, page 388
- Synchronize Cisco voice-mail port with devices, page 393

About Cisco voice-mail port setup

In Cisco Unified Communications Manager Administration, use the Advanced Features > Voice Mail > Cisco Voice Mail Port menu path to configure Cisco voice-mail ports.

The optional Cisco Unity or Cisco Unity Connection software, available as part of Cisco Unified Communications Solutions, provides voice-messaging capability for users when they are unavailable to answer calls. Cisco Unity Connection provides voice-messaging capability for users when they are unavailable to answer calls. This section describes the procedures for adding, configuring, updating, and deleting Cisco voice-mail ports by choosing Voice Mail from the Feature menu of the Cisco Unified Communications Manager Administration window and choosing Cisco Voice Mail Port.

For more information about configuring Cisco Unity, see the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity.

For more information on voice-messaging connectivity to Cisco Unified Communications Manager, see the Cisco Unified Communications Manager System Guide.

Cisco voice-mail ports configuration tips

To connect a Cisco voice-messaging system to Cisco Unified Communications Manager, you must add Cisco voice-mail ports to the Cisco Unified Communications Manager database.
You can also use the Cisco Voice Mail Port Wizard to add a new Cisco voice-mail server and ports or to add multiple ports to an existing server rather than using the procedure that is described here.

### Cisco voice-mail port deletion

When you delete a Cisco voice-mail port that a directory number uses, the number remains in the Cisco Unified Communications Manager database. To determine which directory numbers are using the voice-mail port, in the Voice Mail Port Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

When you delete a voice-mail port that is in use, Cisco Unified Communications Manager displays a message. Before deleting a voice-mail port that is currently in use, you can assign a different voice-mail port to any directory number that is using the voice-mail port that you want to delete.

After you delete the voice-mail port, you can delete the directory number that was using the voice-mail port.

Instead of using the Advanced Features > Voice Mail > Cisco Voice Mail Port menu option, you can use the Cisco Voice Mail Port Wizard to delete ports from an existing server.

### Cisco voice-mail port settings

The following table describes the Cisco voice-mail port settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td></td>
</tr>
</tbody>
</table>
### Cisco voice-mail port settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port Name                  | Enter a name to identify the Cisco voice-mail port. You must add a device for each port on Cisco voice-messaging system. If 24 ports exist, you must define 24 devices. The Port Name field allows 1 to 15 characters, which can include letters, numbers, periods, underscores, and dashes, followed by -VI and the port number.  
**Note** For Cisco Unity, this name must match the name in the Unity Telephony Integration Manager (UTIM), such as Cisco UM-VI1 or Cisco UM-VI2. For Cisco Unity Connection, this name must match the name in Cisco Unity Connection Administration, such as Cisco UM-VI1 or Cisco UM-VI2. |
| Description                | Enter the purpose of the device.                                                                                                                                                                           |
| Device Pool                | Choose the default value or a specific device pool.                                                                                                                                                        |
| Common Device Configuration| Choose the common device configuration to which you want this device assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window. |
| Calling Search Space       | From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that were called from this device. Choose the name of the calling search space that allows calls to the subscriber phones and to any network devices.  
You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 ... button to display the Select Calling Search Space window. Enter a partial calling search space name in the List items where Name contains field. Click the desired calling search space name in the list of 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 CCMAadmin Parameters. |
| AAR Calling Search Space   | Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. |
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 voice-mail port.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this voice-mail port consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the System > Location menu option.

For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.

<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 voice-mail port. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this voice-mail port consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the System &gt; Location menu option. For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Device Security Mode</td>
<td>From the drop-down list box, choose a security mode to apply to the voice-mail server port. The database predefined these options. The default value specifies Not Selected. For more information on configuring security for the voice-mail server, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>
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:

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.
- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

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 *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 *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

### Directory Number Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number</td>
<td>Enter the number that is associated with this voice-mail port. Make sure that this field is unique in combination with the Partition field.</td>
</tr>
<tr>
<td>Partition</td>
<td>Choose the partition to which the directory number belongs. Choose &lt;None&gt; if partitions are not used. If you choose a partition, you must choose a calling search space that includes that 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, then find and choose a partition name. <strong>Note</strong> To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAadmin Parameters.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Calling Search Space       | From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. If you choose a partition, you must choose a calling search space that includes that partition. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name.  
  **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose CCMAadmin Parameters. |
| AAR Group                  | Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted. |
| Internal Caller ID Display | This field indicates text that displays on the called party phone when a call is placed from this line.                                                                                                       |
| Internal Caller ID Display (ASCII format) | This field indicates text that appears on the called party phone, in ASCII format, when a call is placed from this line.                                                                                       |
| External Number Mask       | Specify the mask that is used to format caller ID information for external (outbound) calls. The mask can contain up to 50 characters. Enter the literal digits that you want to display in the caller ID information and use Xs to represent the directory number of the device.  
  You can also enter the international escape character +.  
  When Automated Alternate Routing (AAR) routes calls due to insufficient bandwidth, Cisco Unified Communications Manager uses the value in this field to place the call if sufficient bandwidth is not available.  
  **Example:**  
  DN 1000 (external mask 9728131000) calls DN 1001 (external mask 2144131001). If insufficient bandwidth blocks the call, Cisco Unified Communications Manager uses the AAR prefix digits along with 2144131001 to place the call to 1001. |

**Related Topics**
- Location setup, on page 107
- Search for partition, on page 244
- About calling search space setup, on page 247
- Common device setup, on page 713
Synchronize Cisco voice-mail port with devices

To synchronize devices with a voice mail port that has undergone configuration changes, perform the following procedure, which applies 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 **Advanced Features > Voice Mail > Cisco Voice Mail Port**. The Find and List Voice Mail Ports window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click **Find**. The window displays a list of voice mail ports that match the search criteria.

**Step 4** Check the check boxes next to the voice mail ports with which you want to synchronize affected devices. To choose all voice mail ports in the window, check the check box in the matching records title bar.

**Step 5** Click **Apply Config to Selected**. The Apply Configuration Information dialog displays.

**Step 6** Click **OK**.

Related Topics

- Cisco voice-mail port setup, on page 387
Cisco Voice Mail Port Wizard

This chapter provides information to configure Cisco voice-mail ports in the Cisco Unified Communications Manager database using the Cisco Voice Mail Port Wizard.

For additional information, see the *Cisco Unified Communications Manager System Guide*.

- Voice-mail port setup using wizard, page 395
- Add new Cisco voice-mail server and ports using wizard, page 396
- Add ports to Cisco voice-mail server using wizard, page 400
- Delete ports from Cisco voice-mail server using wizard, page 401

**Voice-mail port setup using wizard**

In Cisco Unified Communications Manager Administration, use the Advanced Features > Voice Mail > Cisco Voice Mail Port Wizard menu path to configure voice-mail ports with the help of a wizard tool.

The optional Cisco Unity or Cisco Unity Connection software, available as part of Cisco Unified Communications Solutions, provides voice-messaging capability for users when they are unavailable to answer calls. This section describes the procedures that are required for adding and configuring Cisco voice-mail ports in Cisco Unified Communications Manager for voice-messaging systems.

For more information about configuring Cisco Unity, see the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity* or the *Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity*.

For more information about configuring Cisco Unity Connection, see the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection* or the *Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection*.

For more information on voice-messaging connectivity to Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

The Cisco Voice Mail Port Wizard tool allows Cisco Unified Communications Manager administrators to quickly add and delete ports that are associated with a Cisco voice-mail server to the Cisco Unified Communications Manager database.
Add new Cisco voice-mail server and ports using wizard

To use the Cisco Voice Mail Port Wizard to add a new Cisco voice-mail server and ports to the Cisco Unified Communications Manager database, perform the following steps.

Before You Begin

The Cisco Voice Mail Port Wizard requires a range of consecutive directory numbers for the voice-mail ports. Make sure the voice-mail pilot number and subsequent numbers are available.

Procedure

Step 1 Choose Advanced Features > Voice Mail > Cisco Voice Mail Port Wizard.
Step 2 Choose Create a new Cisco Voice Mail Server and add ports to it.
Step 3 Click Next.
Step 4 Choose Add ports to a new Cisco Voice Mail server using this name.
Step 5 Enter a name for the Cisco voice-mail server.
   Note For Cisco Unity, this name must match the name in the Unity Telephony Integration Manager (UTIM), such as Cisco UM-VI1 or Cisco UM-VI2. For Cisco Unity Connection, this name must match the name in Cisco Unity Connection Administration, such as Cisco UM-VI1 or Cisco UM-VI2.
Step 6 Click Next.
   The Cisco Voice Mail Ports window displays.
Step 7 From the drop-down list box, choose the number of ports to add.
Step 8 Click Next.
   The Cisco Voice Mail Device Information window displays.
Step 9 Enter the appropriate configuration settings, as described in Table 68: Voice mail port wizard device information configuration settings, on page 397. The wizard applies these configuration settings to all the new ports.
Step 10 Click Next.
   The Cisco Voice Mail Directory Numbers window displays.
Step 11 Enter the directory number settings for the new Cisco voice-mail server as described in Table 69: Voice Mail Port Wizard directory number configuration settings, on page 399.
Step 12 Click Next.
   A window that asks whether you want to add these directory numbers to a line group displays.
Step 13 Choose one of the options that display:
   a) If you choose to add directory numbers to a new line group, skip to Step 14, on page 396.
   b) If you choose to add directory numbers to an existing line group, skip to Step 16, on page 397.
   c) If you choose to add directory numbers to a line group later, skip to Step 18, on page 397.
Step 14 Choose the “Yes. Add directory numbers to a new Line Group” option and click Next.
Step 15 In the Line Group window that displays, enter the name of the new line group and click Next.
   The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.
   Skip to Step 19, on page 397.
**Step 16** Choose the “Yes. Add directory numbers to an existing Line Group” option and click Next.

**Step 17** In the Line Group window that displays, choose a line group from the Line Group Name drop-down list box and click Next.

The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

Skip to **Step 19**, on page 397.

**Step 18** Choose the “No. I will add them later” option and click Next.

The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.

**Step 19** If this information is correct, click Finish to add the new ports.

If the information shown is not correct, click the Back button to edit the information or Cancel to quit without adding any ports.

**Step 20** After the Cisco Voice Mail Port Wizard finishes adding the new voice-mail ports that you specified, the Cisco Voice Mail Port Wizard Results window displays.

The window directs you to the other steps that you need to complete before you can start using these new voice-mail ports.

---

**What to Do Next**

Make sure that you set up the message-waiting indicator (MWI) device. For more information, see topics related to Cisco Unity and Cisco Unity Connection configuration in the *Cisco Unified Communications Manager System Guide*.

**Related Topics**

- [Cisco Voice Mail Port Wizard](#), on page 395
- [Add ports to Cisco voice-mail server using wizard](#), on page 400
- [Delete ports from Cisco voice-mail server using wizard](#), on page 401

---

**Voice Mail Port Wizard device information setup**

The following table describes the Cisco voice-mail port wizard device information configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter the purpose of device.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose the default value Default or any defined device pool.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to which you want this device assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations get configured in the Common Device Configuration window.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. <strong>Note</strong> To set the maximum list box items, choose <strong>System &gt; Enterprise Parameters</strong> and choose CCMAdmin Parameters.</td>
</tr>
<tr>
<td>AAR Calling Search Space</td>
<td>Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.</td>
</tr>
<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 port. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this port consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the <strong>System &gt; Location</strong> menu option. For an explanation of location-based CAC across intercluster trunks, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>Device Security Mode</td>
<td>From the drop-down list box, choose a security mode to apply to the voice-mail server port. The database predefines these options. The default value specifies Not Selected. For more information on configuring security for the voice-mail server, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Location setup, on page 107
- About calling search space setup, on page 247
- Common device setup, on page 713
### Voice Mail Port Wizard directory number setup

The following table describes the Cisco voice-mail port wizard directory number configuration settings.

**Table 69: Voice Mail Port Wizard directory number configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginning Directory Number</td>
<td>Enter the number that people call to access the Cisco voice-mail server. Each new port receives the next available directory number.</td>
</tr>
<tr>
<td>Partition</td>
<td>Choose the partition to which this set of directory numbers belong. Choose None if partitions are not used. If you choose a partition, you must choose a calling search space that includes that 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. Find and choose a partition name by using the procedure in the Search for partition, on page 244. <em>Note</em> To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. If you choose a partition, you must choose a calling search space that includes that partition. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 a calling search space name (see the About calling search space setup, on page 247). <em>Note</em> To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters.</td>
</tr>
<tr>
<td>AAR Group</td>
<td>Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.</td>
</tr>
<tr>
<td>Internal Caller ID Display</td>
<td>This field indicates text that displays on the calling party phone when a call is placed to this line.</td>
</tr>
<tr>
<td>Internal Caller ID Display (ASCII format)</td>
<td>This field indicates text that displays on the calling party phone, in ASCII format, when a call is placed to this line.</td>
</tr>
</tbody>
</table>
Add ports to Cisco voice-mail server using wizard

To use the Cisco Voice Mail Port Wizard to add ports to an existing Cisco voice-mail server, perform the following steps.

Before You Begin

The Cisco Voice Mail Port Wizard requires a range of consecutive directory numbers for the voice-mail ports. Make sure that the voice-mail pilot number and subsequent numbers are available.

The voice-mail pilot number designates the number that people call to access the Cisco voice-mail server.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Advanced Features &gt; Voice Mail &gt; Cisco Voice Mail Port Wizard.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Add ports to an existing Cisco Voice Mail server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Next. The Cisco Voice Mail Server window displays.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the drop-down list box, choose the name of an existing Cisco voice-mail server (pilot number) and click Next. The Cisco Voice Mail Ports window displays and identifies the number of ports that are currently configured.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the drop-down list box, choose the number of ports to add and click Next. The Cisco Voice Mail Directory Numbers window displays the configuration information for the Cisco voice-mail server to which you added the ports. The Cisco Voice Mail Port Wizard automatically selects consecutive directory numbers following the last port and uses the same Partition, Calling Search Space, Display, AAR Group, and External Number Mask settings as the Cisco voice-mail pilot directory number. You can enter a different range of directory numbers in the New Directory Numbers Start at field.</td>
</tr>
<tr>
<td>Step 6</td>
<td>If you need to change the number of ports, click the Back button.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click Next. The Ready to Add Cisco Voice Mail Ports summary window displays. This summary window lists the settings that you configured in the previous windows. The Cisco Voice Mail Port Wizard automatically assigns the correct values for each port.</td>
</tr>
<tr>
<td>Step 8</td>
<td>If this information is correct, click Finish to add the new ports. If the information shown is not correct, click the Back button to edit the information or click Cancel to quit without adding any ports.</td>
</tr>
</tbody>
</table>
Delete ports from Cisco voice-mail server using wizard

To delete ports from an existing Cisco voice-mail server, perform the following steps to use the Cisco Voice Mail Port Wizard.

**Procedure**

**Step 1** Choose Advanced Features > Voice Mail > Cisco Voice Mail Port Wizard.

**Step 2** Choose Delete ports from an existing Cisco Voice Mail server and click Next. The Cisco Voice Mail Server window displays.

**Step 3** From the drop-down list box, choose the name of an existing Cisco voice-mail server (pilot number) and click Next. The Cisco Voice Mail Ports window, which indicates the number of ports that are currently configured, displays.

**Step 4** From the drop-down list box, choose the number of ports to delete and click Next. The Ready to Delete Cisco Voice Mail Ports summary window displays. The summary window provides information about the ports to be deleted. The Cisco Voice Mail Port Wizard automatically updates the port numbers and directory numbers so they are consecutive.

**Step 5** If this information is correct, click Finish to delete the selected ports. If the information shown is not correct, click the Back button to edit the information or to quit without deleting any ports, click Cancel.

**Related Topics**

Cisco Voice Mail Port Wizard, on page 395
Delete ports from Cisco voice-mail server using wizard
Message waiting setup

This chapter provides information about message waiting configuration. For additional information, see topics related to the Voice Mail Connectivity to Cisco Unified Communications Manager in the CiscoUnifiedCommunicationsManagerSystemGuide, as well as topics related to Cisco Unity and Cisco Unity connection.

- About message waiting setup, page 403

About message waiting setup

In Cisco Unified Communications Manager Administration, use the Advanced Features > Voice Mail > Message Waiting menu path to configure message waiting numbers.

The Message Waiting Configuration window allows you to define a message waiting on or message waiting off directory number that a directory-connected based voice-messaging system uses to determine whether to set or clear a message waiting indication for a particular Cisco Unified IP Phone.

Message waiting numbers configuration tips

The voice-messaging system only uses the message-waiting on/off directory number to turn on the message-waiting indicator. Because Cisco Unified Communications Manager does not use the Message Waiting on/off number for receiving calls, the Display, Forward All, Forward Busy, and Forward No Answer fields do not get used.

Message waiting settings

The following table describes the Message Waiting settings.
Table 70: Message waiting settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Waiting Number</td>
<td>Enter the Cisco Message Waiting directory number. Make sure that this number is not used within the Cisco Unified Communications Manager auto-registration range. You may use the following characters: 0 to 9, ?, [, ], +, -, *, ^, #, !. At the beginning of the number, you can enter + if you want to enter the international escape character.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter up to 50 characters for a description of the message-waiting directory number. You may use any characters except the following: &quot;:&quot;, &lt;, &gt;, &amp;.</td>
</tr>
<tr>
<td>Message Waiting Indicator</td>
<td>Click On or Off.</td>
</tr>
<tr>
<td>Partition</td>
<td>If partitions are being used, choose the appropriate partition from the drop-down list box. If you do not want to restrict access to the message-waiting device directory number, choose &lt;None&gt; 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, then find and choose a partition name.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>If partitions and calling search spaces are used, from the drop-down list box, choose a calling search space that includes the partitions of the DNs on all phones whose lamps you want to turn on (the partition that is defined for a phone DN must be in a calling search space that the MWI device uses). You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 a calling search space name (see the About calling search space setup, on page 247).</td>
</tr>
</tbody>
</table>

**Note** To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

**Note** Make sure that the combination of message-waiting device directory number and partition is unique within the Cisco Unified Communications Manager cluster.

Related Topics

Search for partition, on page 244
Message waiting setup, on page 403
Cisco voice-mail pilot setup

This chapter provides information on voice-mail pilot configuration.

For additional information, see topics related to the Voice Mail Connectivity to Cisco Unified Communications Manager in the Cisco Unified Communications Manager System Guide, as well as topics related to Cisco Unity and Cisco Unity connection.

- About voice-mail pilot setup, page 407
- Voice-mail pilot number deletion, page 407
- Voice-mail pilot settings, page 408

About voice-mail pilot setup

In Cisco Unified Communications Manager Administration, use the Advanced Features > Voice Mail > Voice Mail Pilot menu path to configure voice-mail pilots.

The voice mail-pilot number designates the directory number that you dial to access your voice messages. Cisco Unified Communications Manager automatically dials the voice-messaging number when you press the Messages button on your phone. Each pilot number can belong to a different voice-messaging system.

Voice-mail pilot number deletion

To delete the voice-mail pilot number, perform these procedures. You cannot delete the default or the No Voice Mail profile numbers.

Note

If you choose the default or the No Voice Mail pilot numbers, the Delete button does not display.

You cannot delete voice-mail pilot numbers that a voice-mail profile uses. To find out which voice-mail profiles are using the voice-mail pilot, in the Voice Mail Pilot Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a voice-mail pilot that is in use, Cisco Unified Communications Manager displays a message. Before deleting a voice-mail pilot that is currently in use, you must perform either or both of the following tasks:
• Assign a different voice-mail pilot to any voice-mail profiles that are using the voice-mail pilot that you want to delete.

• Delete the voice-mail profiles that are using the voice-mail pilot that you want to delete.

If a voice-mail profile uses this voice-mail pilot number, a message displays and indicates the number of voice-mail profiles that use this voice-mail pilot number.

**Related Topics**
- About voice-mail profile setup, on page 411
- Voice-mail profile deletion, on page 411
- Access dependency records, on page 874

---

**Voice-mail pilot settings**

The following table describes the voice-mail pilot settings.

**Table 71: Voice-mail pilot settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Mail Pilot Number</td>
<td>Enter a number to identify the voice mail pilot number. Allowed characters are numeric (0-9), plus (+), asterisk (*), and pound (#).</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this pilot number.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the pilot number. 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>
<tr>
<td>Make this the default</td>
<td>Check the check box to make this pilot number the default Voice Mail Pilot for the system.</td>
</tr>
<tr>
<td>Voice Mail Pilot for the</td>
<td></td>
</tr>
<tr>
<td>system</td>
<td></td>
</tr>
</tbody>
</table>

**Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose CCMAadmin Parameters.

**Related Topics**
- About calling search space setup, on page 247
Cisco voice-mail pilot setup, on page 407
Voice-mail pilot settings
Voice-mail profile setup

This chapter provides information about voice-mail profile configuration.

For additional information, see topics related to the Voice Mail Connectivity to Cisco Unified Communications Manager in the *Cisco Unified Communications Manager System Guide*, as well as topics related to Cisco Unity and Cisco Unity connection.

- About voice-mail profile setup, page 411
- Voice-mail profile deletion, page 411
- Voice-mail profile settings, page 412
- Synchronize voice-mail profile with devices, page 413

About voice-mail profile setup

In Cisco Unified Communications Manager Administration, use the **Advanced Features > Voice Mail > Voice Mail Profile** menu path to configure voice-mail profiles.

The Voice Mail Profile Configuration window of Cisco Unified Communications Manager Administration allows you to define any line-related voice-messaging information.

**Voice-mail profiles configuration tips**

A voice-mail profile gets assigned to a directory number, not to a device.

**Related Topics**

- Synchronize voice-mail profile with devices, on page 413

Voice-mail profile deletion

You cannot delete the default profile or the No Voice Mail profile.

You cannot delete a voice-mail profile that a directory number uses. To find out which directory numbers are using the voice-mail profiles, in the Voice Mail Profile Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a voice-mail profile
that is in use, Cisco Unified Communications Manager displays a message. Before deleting a voice-mail profile that is currently in use, you must perform either or both of the following tasks:

- Assign a different voice-mail profile to any devices that are using the voice-mail profile that you want to delete.
- Delete the devices that are using the voice-mail profile that you want to delete.

**Related Topics**

*Access dependency records, on page 874*

---

**Voice-mail profile settings**

The following table describes the voice-mail profile settings.

**Table 72: Voice mail profile settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice Mail Profile Information</td>
<td>Enter a name to identify the voice-mail profile. Valid characters comprise alphanumeric characters (a-z, A-Z, 0-9), period(,), dash(-), underscore(_).</td>
</tr>
<tr>
<td>Voice Mail Profile Name</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;), back-slash (), angle brackets (&lt;&gt;), dollar sign ($), single-quote (‘), open paren ( [ ), close paren ( ] ), slash (/), colon (:), semi-colon (;), equal sign (=), at sign (@), tilde (~), brackets { }, or apostrophe (‘).</td>
</tr>
<tr>
<td>Description</td>
<td>Set the appropriate voice-mail pilot number that is defined in the Voice Mail Pilot Configuration or Use Default.</td>
</tr>
<tr>
<td>Voice Mail Pilot</td>
<td>Specify the mask that is used to format the voice mailbox number for auto-registered phones. When a call is forwarded to a voice-messaging system from a directory line on an auto-registered phone, Cisco Unified Communications Manager applies this mask to the number that is configured in the Voice Mail Box field for that directory line. For example, if you specify a mask of 972813XXXX, the voice mailbox number for directory number 7253 becomes 9728137253. If you do not enter a mask, the voice mailbox number matches the directory number (7253 in this example). By default, Cisco Unified CM sets the voice mailbox number to the same value as the directory number. You can change the voice mailbox number when you are configuring the directory number. <strong>Note</strong> When a call gets redirected from a DN to a voice-mail server/service that is integrated with Cisco Unified CM using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP diversion header. This behavior is expected because the diversion header gets used by the Cisco Unified CM server to choose a mailbox.</td>
</tr>
</tbody>
</table>
Synchronize voice-mail profile with devices

To synchronize devices with a voice mail profile that has undergone configuration changes, perform the following procedure, which applies 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 **Advanced Features > Voice Mail > Voice Mail Profile**. The Find and List Voice Mail Profiles window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find. The window displays a list of voice mail profiles that match the search criteria.

Step 4 Click the voice mail profile to which you want to synchronize applicable devices. The Voice Mail Profile Configuration screen 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.

Related Topics

Voice-mail profile setup, on page 411
Synchronize voice-mail profile with devices
Other advanced features menu options

This chapter provides brief descriptions of selected Advanced Features menu options. A pointer to the document that contains greater details for each Advanced Features menu option is provided.

- SAF (Call Control Discovery), page 415
- Cisco Extension Mobility Cross Cluster, page 415
- Cisco Intercompany Media Engine, page 416
- Fallback setup, page 416
- Called Party Tracing, page 416
- VPN setup, page 416

SAF (Call Control Discovery)

In Cisco Unified Communications Manager Administration, use the submenus under the Advanced Features > SAF menu path to configure 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 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.

For more information, see the VPN setup, on page 416 chapter in the Cisco Unified Communications Manager Features and Services Guide.

Cisco Extension Mobility Cross Cluster

In Cisco Unified Communications Manager Administration, use the submenus under the Advanced Features > EMCC menu path to configure the Cisco Extension Mobility Cross Cluster feature.
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.

For more information, see the *Cisco Unified Communications Manager Features and Services Guide*.

---

**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.

---

**Cisco Intercompany Media Engine**

In Cisco Unified Communications Manager Administration, use the submenus under the *Advanced Features > Intercompany Media Services* menu path to configure the Cisco Intercompany Media Engine.

Cisco Intercompany Media Engine provides a technique for establishing direct IP connectivity between enterprises by combining peer-to-peer technologies with the existing public switched telephone network (PSTN) infrastructure. Cisco Intercompany Media Engine allows companies that have deployed Cisco Unified Communications Manager to communicate over the Internet rather than the PSTN by creating dynamic Session Initiation Protocol (SIP) trunks between the enterprises.

For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

---

**Fallback setup**

In Cisco Unified Communications Manager Administration, use the submenus under the *Advanced Features > Fallback* menu path to configure fallback information.

Cisco Intercompany Media Engine configuration comprises configuration of fallback information.

For more information, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

---

**Called Party Tracing**

In Cisco Unified Communications Manager Administration, use the submenus under the *Advanced Features > Called Party Tracing* menu path to configure Called Party Tracing feature.

Called Party Tracing allows you to configure a directory number or list of directory numbers that you want to trace. You can request on-demand tracing of calls using the Session Trace Tool.

For more information, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

---

**VPN setup**

**Note**

The VPN menu and its options are not available in the U.S. export unrestricted version of Cisco Unified Communications Manager.
In Cisco Unified Communications Manager Administration, use the submenus under the Advanced Features > VPN menu path to configure the VPN feature.

The Cisco VPN Client for Cisco Unified IP Phones adds another option for customers attempting to solve the remote telecommuter problem by complementing other Cisco remote telecommuting offerings.

For more information, see the Cisco Unified Communications Manager Security Guide.
VPN setup
PART VI

Device setup

• CTI route point setup, page 421
• Gatekeeper setup, page 429
• Gateway setup, page 433
• Cisco Unified IP Phone setup, page 537
• Trunk setup, page 591
• Device defaults setup, page 651
• Device firmware load information, page 655
• Default device profile setup, page 657
• Device profile setup, page 663
• Phone button template setup, page 671
• Softkey template setup, page 675
• IP phone services setup, page 683
• SIP profile setup, page 695
• Common device setup, page 713
• Common phone profile setup, page 721
• Feature Control Policy setup, page 727
• Recording Profile setup, page 731
• SIP normalization script setup, page 733
• Other device menu options, page 739
CTI route point setup

This chapter provides information to configure CTI route points and CTI ports. For additional information, see topics related to computer telephony integration and trusted relay points in the Cisco Unified Communications Manager System Guide.

- About CTI route point setup, page 421
- CTI route point setup, page 422
- CTI route point deletions, page 422
- CTI route point settings, page 423
- Synchronize CTI route point, page 426

About CTI route point setup

A computer telephony integration (CTI) route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

For first-party call control, you can optionally add a CTI port for each active voice line (the CTI application determines this). Applications that use CTI route points and CTI ports include Cisco IP Softphone, Cisco Unified Communications Manager Auto-Attendant, and Cisco IP Interactive Voice Response System. After you add a CTI route point to Cisco Unified Communications Manager Administration, information from the RIS Data Collector service displays in the CTI Route Point Configuration window. When available, the IP address of the device and the name of the Cisco Unified Communications Manager with which the device registered display.

Note

You must not associate CTI route points with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists. If a DN is a member of a line group or hunt list, you cannot associate that DN with a CTI route point that you configure with the CTI Route Point Configuration window.

For detailed instructions on how to configure CTI route points and CTI ports that are associated with these applications, see the documentation and online help that is included with these applications.
CTI route point setup

In Cisco Unified Communications Manager Administration, use the **Device > CTI Route Point** menu path to configure CTI route points.

A computer telephony integration (CTI) route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

For first-party call control, you can optionally add a CTI port for each active voice line (the CTI application determines this). Applications that use CTI route points and CTI ports include Cisco IP Softphone, Cisco Unified Communications Manager Auto-Attendant, and Cisco IP Interactive Voice Response System. After you add a CTI route point to Cisco Unified Communications Manager Administration, information from the RIS Data Collector service displays in the CTI Route Point Configuration window. When available, the IP address of the device and the name of the Cisco Unified Communications Manager with which the device registered display.

---

**Note**

You must not associate CTI route points with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists. If a DN is a member of a line group or hunt list, you cannot associate that DN with a CTI route point that you configure with the CTI Route Point Configuration window.

For detailed instructions on how to configure CTI route points and CTI ports that are associated with these applications, see the documentation and online help that is included with these applications.

---

**CTI route point configuration tips**

After you add a CTI route point to Cisco Unified Communications Manager Administration, information from the RIS Data Collector service displays in the CTI Route Point Configuration window. When available, the device IP address and the name of the Cisco Unified Communications Manager with which the device registered display.

You can add and configure directory numbers for a CTI route point.

For instructions on how to reset a CTI route point, see the descriptions of the Reset Selected and Reset buttons.

---

**Related Topics**

- GUI buttons and icons, on page 18
- About directory number setup, on page 263
- Synchronize CTI route point, on page 426

---

**CTI route point deletions**

Because you can delete a CTI route point that is assigned to one or more directory numbers, you should determine which directory numbers are using the CTI route point. To determine which directory numbers are using the CTI route point, choose Dependency Records link from the Related Links drop-down list box in the CTI Route Point Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a CTI route point that is in use, Cisco Unified Communications Manager displays a message.
If you delete a CTI Route Point that has a directory number assigned to it, you can find the directory number by using the Route Plan Report. You can also delete the directory number by using the Route Plan Report.

Related Topics

Access dependency records, on page 874

CTI route point settings

The following table describes the CTI route point settings.

Table 73: CTI route point settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter unique identifier for this device, from 1 to 15 characters, including alphanumeric, dot, dash, or underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the CTI route point. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose the name of a Device Pool. The device pool specifies the collection of properties for this device, including Cisco Unified Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to which you want this CTI route point assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Configure common device configurations in the Common Device Configuration window.</td>
</tr>
</tbody>
</table>
| Calling Search Space       | From the drop-down list box, choose a calling search space. The calling search space specifies the collection of partitions that are searched to determine how a collected (originating) number should be routed.  
You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name.  
*Note* To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters. |

Cisco Unified Communications Manager Administration Guide, Release 9.1(1)
### Field | Description
--- | ---
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 CTI route point.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this CTI route point consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the **System > Location** menu option.

For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

User Locale | From the drop-down list box, choose the locale that is associated with the CTI route point. The user locale identifies a set of detailed information to support users, including language and font.

Cisco Unified Communications Manager makes this field available only for CTI route points 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 that information be displayed (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 Manager locale installer that is in the *Cisco Unified Communications Operating System Administration Guide*.

Media Resource Group List | Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List.

If you choose <none>, Cisco Unified Communications Manager uses the Media Resource Group that is defined in the device pool.

For more information, see topics related to media resource management in the *Cisco Unified Communications Manager System Guide*.

Network Hold MOH Audio Source | To specify the audio source that plays when the network initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays.

If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID.

You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources > Music On Hold Audio Source**.
To specify the audio source that plays when an application initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID.

You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources > Music On Hold Audio Source**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| User Hold MOH Audio Source | 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:  
  • Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.  
  • Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  • On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
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 RSVP Agent).  
If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the *Cisco Unified Communications Manager System Guide* for details of call behavior.  
If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVP Agent 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 *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
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.

**Tip** 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.

<table>
<thead>
<tr>
<th>Field</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. <strong>Tip</strong> 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>Geolocation</td>
<td>From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the System &gt; Geolocation Configuration menu option. For an explanation of geolocations, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide. For an overview and details of how logical partitioning uses geolocations, see the Cisco Unified Communications Manager Features and Services Guide.</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 CTI Route Point Configuration window.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Location setup, on page 107
- About calling search space setup, on page 247
- CTI route point setup, on page 421
- Common device setup, on page 713

**Synchronize CTI route point**

To synchronize a CTI route point with the most recent configuration changes, perform the following procedure, which applies 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 Device > CTI Route Point. The Find and List CTI Route Points window displays.
2. **Step 2** Choose the search criteria to use.
3. **Step 3** Click Find.
The window displays a list of CTI route points that match the search criteria.

**Step 4** Check the check boxes next to the CTI route points that you want to synchronize. To choose all CTI route points in the window, check the check box in the matching records title bar.

**Step 5** Click Apply Config to Selected. The Apply Configuration Information dialog displays.

**Step 6** Click OK.

**Related Topics**

CTI route point setup, on page 421
Synchronize CTI route point
CHAPTER 67

Gatekeeper setup

This chapter provides information about gatekeeper configuration using Cisco Unified Communications Manager Administration.

For additional information about gatekeepers and trunks, see the following Cisco documentation:

- Cisco Unified Communications Manager System Guide
- Cisco Unified Communications Solution Reference Network Design (SRND)
- Cisco IOS Multimedia Conference Manager (Command Reference) documentation

- About gatekeeper setup, page 429
- Gatekeeper reset, page 430
- Gatekeeper deletions, page 430
- Gatekeeper settings, page 431
- Synchronize gatekeeper, page 432

About gatekeeper setup

In Cisco Unified Communications Manager Administration, use the Device > Gatekeeper menu path to configure gatekeepers.

A gatekeeper device, also known as a Cisco Multimedia Conference Manager (MCM), supports the H.225 Registration, Admission, and Status Protocol (RAS) message set that is used for call admission control, bandwidth allocation, and dial pattern resolution (call routing). The gatekeeper provides these services for communications between Cisco Unified Communications Manager clusters and H.323 networks. You can configure multiple gatekeeper devices per Cisco Unified Communications Manager cluster. You can configure alternate gatekeepers for redundancy. See the Cisco Multimedia Conference Manager (MCM) documentation and the Cisco Unified Communications Solution Reference Network Design (SRND) for alternate gatekeeper configuration details.

Gatekeeper configuration comprises components:

- Cisco Unified Communications Manager configuration. Each Cisco Unified Communications Manager cluster can register with one or more gatekeepers. This chapter describes how to configure the gatekeeper
in Cisco Unified Communications Manager. You also need to configure trunk devices on the Trunk Configuration window.

- Gatekeeper configuration on the router. This type of configuration applies to a Cisco IOS Multimedia Conference Manager (MCM) that acts as the gatekeeper. Recommended platforms for the gatekeeper include Cisco 2600, 3600, or 7200 routers with Cisco IOS Release 12.1(3)T or higher. See the MCM documentation for information on configuring the gatekeeper. Alternate gatekeeper configuration occurs in the MCM only, so no configuration is necessary in Cisco Unified Communications Manager.

---

**Note**

You can configure multiple gatekeeper devices per Cisco Unified Communications Manager cluster.

---

### Gatekeepers configuration tips

You can configure multiple gatekeeper devices per Cisco Unified Communications Manager cluster.

---

**Related Topics**

- **Trunk setup** on page 591

---

### Gatekeeper reset

Resetting a gatekeeper does not mean that the physical device is reset; instead, resetting forces the Cisco Unified Communications Manager to reset the logical connection to the gatekeeper and to reregister with the gatekeeper. During this time of reregistering and until successful registration, new calls that are made by using this trunk, which uses this gatekeeper, fail.

When you reset a gatekeeper, the Cisco Unified Communications Manager cluster unregisters (URQ) and then reregisters (RRQ) with the gatekeeper.

For instructions on how to reset a gatekeeper, see the descriptions of the Reset Selected and Reset buttons.

---

**Note**

Resetting a gatekeeper does not cause all active calls that this gatekeeper controls to be dropped; however, new call attempts fail.

---

**Related Topics**

- **GUI buttons and icons** on page 18
- **Synchronize gatekeeper** on page 432

---

### Gatekeeper deletions

You cannot delete a gatekeeper that is assigned to one or more trunks. To find out which trunks are using the gatekeeper, choose Dependency Records from the Related Links drop-down list box that is on the Gatekeeper 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. If you try to delete a gatekeeper that is in use, Cisco Unified Communications Manager displays an error message. Before deleting a gatekeeper that is currently in use, you must perform either or both of the following tasks:
• Assign a different gatekeeper to any trunks that are using the gatekeeper that you want to delete.
• Delete the trunks that are using the gatekeeper that you want to delete.

**Related Topics**

- Set up trunk, on page 646
- Delete trunk, on page 647
- Access dependency records, on page 874

## Gatekeeper settings

The following table describes the gatekeeper settings.

### Table 74: Gatekeeper settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gatekeeper Information</strong></td>
<td></td>
</tr>
<tr>
<td>Host Name/IP Address</td>
<td>Enter the IP address or host name of the gatekeeper in this required field. You can register multiple gatekeepers per Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the gatekeeper. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Registration Request Time to Live</td>
<td>Do not change this value unless a Cisco TAC engineer instructs you to do so. Enter the time in seconds. The default value specifies 60 seconds. The Registration Request Time to Live field indicates the time that the gatekeeper considers a registration request (RRQ) valid. The system must send a keepalive RRQ to the gatekeeper before the RRQ Time to Live expires. Cisco Unified Communications Manager sends an RRQ to the gatekeeper to register and subsequently to maintain a connection with the gatekeeper. The gatekeeper may confirm (RCF) or deny (RRJ) the request.</td>
</tr>
<tr>
<td>Registration Retry Timeout</td>
<td>Do not change this value unless a Cisco TAC engineer instructs you to do so. Enter the time in seconds. The default value specifies 300 seconds. The Registration Retry Timeout field indicates the time that Cisco Unified Communications Manager waits before retrying gatekeeper registration after a failed registration attempt.</td>
</tr>
<tr>
<td>Enable Device</td>
<td>This check box allows you to register this gatekeeper with Cisco Unified Communications Manager. By default, this check box remains checked. To unregister the gatekeeper from Cisco Unified Communications Manager gracefully, uncheck this check box. The gatekeeper unregisters within approximately 1 minute of updating this field.</td>
</tr>
</tbody>
</table>
Related Topics

Gatekeeper setup, on page 429

Synchronize gatekeeper

To synchronize a gatekeeper with the most recent configuration changes, perform the following procedure, which applies 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 Device > Gatekeeper.  
The Find and List Gatekeepers window displays.

**Step 2**  Choose the search criteria to use.

**Step 3**  Click Find.  
The window displays a list of gatekeepers that match the search criteria.

**Step 4**  Check the check boxes next to the gatekeepers that you want to synchronize. To choose all gatekeepers in the window, check the check box in the matching records title bar.

**Step 5**  Click Apply Config to Selected.  
The Apply Configuration Information dialog displays.

**Step 6**  Click OK.

---

Related Topics

Gatekeeper setup, on page 429
CHAPTER 68

Gateway setup

This chapter provides information about using Cisco Unified Communications Manager for working with and configuring Cisco gateways.

• About gateway setup, page 433
• Gateway reset, page 434
• Gateway deletion, page 434
• Cisco Unified Communications gateway settings, page 435
• Port setup, page 467
• Add gateway to Cisco Unified Communications Manager, page 522
• Gateway and port modification, page 534

About gateway setup

In Cisco Unified Communications Manager Administration, use the Device > Gateway menu path to configure gateways.

Cisco Unified Communications gateways enable Cisco Unified Communications Manager to communicate with non-IP telecommunications devices.

Related Topics

- MGCP gateway settings, on page 435
- H.323 gateway settings, on page 438
- Analog access gateway settings, on page 458
- Cisco VG248 gateway settings, on page 463
- Cisco IOS SCCP gateway settings, on page 464
- Port setup, on page 467
- Add gateway to Cisco Unified Communications Manager, on page 522
Gateway reset

For instructions on how to reset a gateway, see the descriptions of the Reset Selected and Reset buttons.

Note
Restarting or resetting an H.323 gateway does not physically restart/reset the gateway; it only reinitializes the configuration that was loaded by Cisco Unified Communications Manager. When you reset any other gateway type, Cisco Unified Communications Manager automatically drops the calls that are using the gateway. When you restart any other gateway type, Cisco Unified Communications Manager attempts to preserve the calls that are using the gateway.

Related Topics
- GUI buttons and icons, on page 18
- Synchronize gateway, on page 534

Gateway deletion

Gateways and ports use a variety of configuration information such as partitions, device pools, and directory numbers. Before updating or deleting gateways or ports, you can find configuration information about that gateway and port by using the Dependency Records link. To access the link, choose Dependency Records from the Related Links drop-down list box and click Go.

If you try to delete a gateway that a route group is using, Cisco Unified Communications Manager displays a message. To find out which route groups are using the gateway, choose Dependency Records from the Related Links drop-down list box in the Gateway Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. Before deleting a gateway that is currently in use, you must perform either or both of the following tasks:

• Assign a different gateway to any route groups that are using the gateway that you want to delete.
• Delete the route groups that are using the gateway that you want to delete.

Note
For each gateway type, the Gateway Configuration window displays either Device is trusted or Device is not trusted, along with a corresponding icon. The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Related Topics
- Route group deletion, on page 178
- Add devices to route group, on page 180
- Dependency records, on page 873
- Access dependency records, on page 874
Cisco Unified Communications gateway settings

Cisco Unified Communications gateways enable Cisco Unified Communications Manager to communicate with non-IP telecommunications devices.

For each gateway type, the Gateway Configuration window displays either Device is trusted or Device is not trusted, along with a corresponding icon. The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Related Topics

Port setup, on page 467

MGCP gateway settings

The following table provides detailed descriptions for MGCP gateway configuration settings.

Table 75: MGCP gateway configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Details</td>
<td>Enter a name of up to 64 characters that identifies the Cisco MGCP gateway. Use the Domain Name Service (DNS) host name if it is configured to resolve correctly; otherwise, use the host name as defined on the Cisco MGCP gateway. If you are using the host name as it is configured on the IOS gateway, the name that you enter here must match exactly. For example, if the hostname is configured on the gateway to resolve to vg200-1 and the IP domain name is not configured, enter the hostname in this field (in this case, vg200-1). If the hostname is configured on the gateway as vg200-1 and the IP domain name is configured on the gateway as cisco.com, enter vg200-1.cisco.com in this field.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Description</td>
<td>From the drop-down list box, choose a Cisco Unified Communications Manager redundancy group.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Group</td>
<td>A Cisco Unified Communications Manager redundancy group includes a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager. If the primary Cisco Unified Communications Manager is not available or fails, the gateway attempts to connect with the next Cisco Unified Communications Manager in the list and so on.</td>
</tr>
</tbody>
</table>
You must specify the beginning port number for some VICs. For example, if the VIC in Subunit 0 begins at 0 and has two ports (0 and 1), the VIC in Subunit 1 must begin at a port number greater than 1 and have two ports (2 and 3 or 4 and 5).

The correct number of slots displays for each model of MGCP gateway. (The VG200 gateway has only one slot.)

To begin configuring ports on a module, select the module first; then, click Save.
For each available slot on the MGCP gateway, choose the type of module that is installed; for example:

- **NM-1V**—Has one voice interface card (VIC) in Subunit 0 for FXS or FXO. When you use the VIC-2BRI-S/T-TE card with a NM-1V module, you can make two calls because the second BRI port is shut down.

- **NM-2V**—Has two VICs, one in Subunit 0 and one in Subunit 1 for either FXS or FXO. When you use the VIC-2BRI-S/T-TE card with a NM-2V module, you can make four calls. If another VIC is in the second slot of the NM-2V, the second port on the VIC-2BRI-S/T-TE gets shut down.

- **NM-HDV**—Has one VIC in Subunit 0 for either T1-CAS or T1-PRI, or E1-PRI.

- **NM-HDA**—Has three VICs, one in Subunit 0, one in Subunit 1, and one in Subunit 2.

- **VWIC-SLOT**—Has a slot for any of the following modules: VIC (FXS, FXO, or BRI), T1-CAS, T1-PRI, or E1-PRI.

- **AIM-VOICE-30**—Has two VICs, one in Subunit 0 and one in Subunit 1 for T1-CAS, T1-PRI, or E1-PRI.

- **WS-X6600-24FXS**—Has 24 FXS ports.

- **WS-X6600-6T1**—Has six ports for T1 PRI or CAS.

- **WS-X6600-6E1**—Has six ports for E1 PRI.

- **WS-SVC-CMM-MS**—Has two port adapters, one for a T1 interface and one for an E1 interface for Europe and other countries.

- **None**—Has no network modules installed.

If you configure the Cisco 881 or the Cisco 888/887/886 for MGCP in the Gateway Configuration window, choose the following options when you configure the subunits:

For Cisco 881

- Subunit 1 - VIC3-4FXS-DID
- Subunit 3 - VIC2-1FXO

For Cisco 888/887/886

- Subunit 1 - VIC3-4FXS-DID
- Subunit 2 - VIC2-1BRI

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Module in Slot 0 Module in Slot 1 Module in Slot 2 Module in Slot 3 (and so on) | For each available slot on the MGCP gateway, choose the type of module that is installed; for example:  
- **NM-1V**—Has one voice interface card (VIC) in Subunit 0 for FXS or FXO. When you use the VIC-2BRI-S/T-TE card with a NM-1V module, you can make two calls because the second BRI port is shut down.  
- **NM-2V**—Has two VICs, one in Subunit 0 and one in Subunit 1 for either FXS or FXO. When you use the VIC-2BRI-S/T-TE card with a NM-2V module, you can make four calls. If another VIC is in the second slot of the NM-2V, the second port on the VIC-2BRI-S/T-TE gets shut down.  
- **NM-HDV**—Has one VIC in Subunit 0 for either T1-CAS or T1-PRI, or E1-PRI.  
- **NM-HDA**—Has three VICs, one in Subunit 0, one in Subunit 1, and one in Subunit 2.  
- **VWIC-SLOT**—Has a slot for any of the following modules: VIC (FXS, FXO, or BRI), T1-CAS, T1-PRI, or E1-PRI.  
- **AIM-VOICE-30**—Has two VICs, one in Subunit 0 and one in Subunit 1 for T1-CAS, T1-PRI, or E1-PRI.  
- **WS-X6600-24FXS**—Has 24 FXS ports.  
- **WS-X6600-6T1**—Has six ports for T1 PRI or CAS.  
- **WS-X6600-6E1**—Has six ports for E1 PRI.  
- **WS-SVC-CMM-MS**—Has two port adapters, one for a T1 interface and one for an E1 interface for Europe and other countries.  
- **None**—Has no network modules installed.  

If you configure the Cisco 881 or the Cisco 888/887/886 for MGCP in the Gateway Configuration window, choose the following options when you configure the subunits:  
For Cisco 881  
- Subunit 1 - VIC3-4FXS-DID  
- Subunit 3 - VIC2-1FXO  

For Cisco 888/887/886  
- Subunit 1 - VIC3-4FXS-DID  
- Subunit 2 - VIC2-1BRI  

Product-Specific Configuration
The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice.

To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box.

If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

### H.323 gateway settings

After a gateway is registered with Cisco Unified Communications Manager, gateway registration status may display in Cisco Unified Communications Manager Administration as unknown.

The following table lists configuration settings for H.323 gateways.

Table 76: H.323 gateway configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Enter a unique name that Cisco Unified Communications Manager uses to identify the device. Use either the IP address or the host name as the device name.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Device Pool</td>
<td>From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>From the drop-down list box, choose the common device configuration you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call Classification</td>
<td>This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet).</td>
</tr>
<tr>
<td></td>
<td>When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet.</td>
</tr>
<tr>
<td></td>
<td>This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, among the available media resources according to the priority order that a Media Resource Group List defines.</td>
</tr>
<tr>
<td>Packet Capture Mode</td>
<td>Configure this field only when you need to troubleshoot encrypted signaling information for the H.323 gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Packet Capture Duration</td>
<td>Configure this field only when you need to troubleshoot encrypted signaling information for the H.323 gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<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.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, choose the appropriate location for this device.</td>
</tr>
<tr>
<td></td>
<td>A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.</td>
</tr>
<tr>
<td></td>
<td>To configure a new location, use the System &gt; Location menu option.</td>
</tr>
<tr>
<td></td>
<td>For an explanation of location-based CAC across intercluster trunks, see topics related to location configuration in the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>AAR Group</td>
<td>Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.</td>
</tr>
</tbody>
</table>
Choose the QSIG option if you want to use H.323 gateways to transport (tunnel) non-H.323 protocol information in H.323 signaling messages from Cisco Unified Communications Manager to other Annex M.1-compliant H.323 PINXs. QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and Path Replacement.

Note
See the [Cisco Unified Communications Manager Software Compatibility Matrix](#) for information about Annex M.1 feature compatibility with third-party vendor(s).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunneled Protocol</td>
<td>Choose the QSIG option if you want to use H.323 gateways to transport (tunnel) non-H.323 protocol information in H.323 signaling messages from Cisco Unified Communications Manager to other Annex M.1-compliant H.323 PINXs. QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and Path Replacement. Note: See the Cisco Unified Communications Manager Software Compatibility Matrix for information about Annex M.1 feature compatibility with third-party vendor(s).</td>
</tr>
<tr>
<td>QSIG Variant</td>
<td>To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, choose one of the following options. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise. • No Changes • Not Selected • ECMA—If the QSIG Variant is set to ECMA (Protocol Profile 0x91), ensure that the ASN.1 Rose OID Encoding service parameter is set to Use Global Value (ECMA). • ISO—(Default) If the QSIG Variant is set to ISO (Protocol Profile 0x9F), ensure that the ASN.1 Rose OID Encoding service parameter is set to either Use Local Value or Use Global Value (ISO). For more information, see the following information: • Be aware that the QSIG Variant can also be defined as a clusterwide parameter. • For information on QSIG support with Cisco Unified Communications Manager, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>
To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box.

This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations.

From the drop-down list box, choose one of the following options:

- No Changes.
- Not Selected
- Use Global Value (ISO)—Select this option only if the connected PBX does not support Local Value.
- Use Global Value (ECMA)—Select this option only if the QSIG Variant service parameter is set to ECMA (Protocol Profile 0x91).
- Use Local Value—(Default) Use this option that is supported by most telephony systems when the QSIG Variant service parameter is set to ISO (Protocol Profile 0x9F).

For more information, see the following information:

- Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter.
- For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN.1 ROSE OID Encoding</td>
<td>To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box.</td>
</tr>
<tr>
<td></td>
<td>This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• No Changes.</td>
</tr>
<tr>
<td></td>
<td>• Not Selected</td>
</tr>
<tr>
<td></td>
<td>• Use Global Value (ISO)—Select this option only if the connected PBX does not support Local Value.</td>
</tr>
<tr>
<td></td>
<td>• Use Global Value (ECMA)—Select this option only if the QSIG Variant service parameter is set to ECMA (Protocol Profile 0x91).</td>
</tr>
<tr>
<td></td>
<td>• Use Local Value—(Default) Use this option that is supported by most telephony systems when the QSIG Variant service parameter is set to ISO (Protocol Profile 0x9F).</td>
</tr>
<tr>
<td></td>
<td>For more information, see the following information:</td>
</tr>
<tr>
<td></td>
<td>• Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter.</td>
</tr>
<tr>
<td></td>
<td>• For information on QSIG support with Cisco Unified Communications Manager, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
</tbody>
</table>
From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.
- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

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 RSVP Agent).

If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the Cisco Unified Communications Manager System Guide for details of call behavior.

If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVP Agent 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 Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.

### Field: Use Trusted Relay Point

#### Description:
From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.
- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

### Field: Signaling Port

#### Description:
This field applies only to H.323 devices. The value designates the H.225 signaling port that this device uses.

**Default value:** 1720. **Valid values:** range from 1 to 65535.

### Field: Media Termination Point Required

#### Description:
If you want a Media Termination Point to implement features that H.323 does not support (such as hold and transfer), check the check box.

Use this check box only for H.323 clients and H.323 devices that do not support the H.245 Empty Capabilities Set message.

If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry Video Call as Audio</td>
<td>This check box applies only to video endpoints that receive a call. By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control. Call control reroutes the call within the route/hunt list. If Automatic Alternate Routing (AAR) is configured and enabled, call control also reroutes the call between route/hunt lists.</td>
</tr>
<tr>
<td>Wait for Far End H.245 Terminal Capability Set</td>
<td>This field applies only to H.323 devices. By default, system checks this check box to specify that Cisco Unified Communications Manager needs to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. Unchecking this check box specifies that Cisco Unified Communications Manager should initiate capabilities exchange.</td>
</tr>
<tr>
<td>Path Replacement Support</td>
<td>This check box displays if you choose the QSIG option from the Tunneled Protocol drop-down list box. This setting works with QSIG tunneling (Annex M.1) to ensure that non-H.323 information gets sent on the leg of the call that uses path replacement.</td>
</tr>
<tr>
<td>Transmit UTF-8 for Calling Party Name</td>
<td>This device uses the user locale setting of the device pool of the device to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device pool of the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool of the device. If the user locale setting matches the terminating phone user locale, the phone displays the characters.</td>
</tr>
<tr>
<td>SRTP Allowed</td>
<td>Check the SRTP Allowed check box if you want Cisco Unified Communications Manager to allow secure and nonsecure calls over the gateway. If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the gateway and uses RTP.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>H.235 Pass Through Allowed</td>
<td>This feature allows Cisco Unified Communications Manager to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel. To allow H.235 pass through, check the check box.</td>
</tr>
</tbody>
</table>

Multilevel Precedence and Preemption (MLPP) Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Domain</td>
<td>From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value &lt;None&gt;, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
<tr>
<td>MLPP Indication</td>
<td>This device type does not have this setting.</td>
</tr>
<tr>
<td>MLPP Preemption</td>
<td>This device type does not have this setting.</td>
</tr>
</tbody>
</table>

Call Routing Information - Inbound Calls

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant Digits</td>
<td>Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls coming into the device. Choose the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number called.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the appropriate calling search space. A calling search space specifies the collection of Route Partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. Note: To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAdmin Parameters.</td>
</tr>
<tr>
<td>AAR Calling Search Space</td>
<td>Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.</td>
</tr>
<tr>
<td>Prefix DN</td>
<td>Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +.</td>
</tr>
</tbody>
</table>
### Field Description

**Redirecting Number IE Delivery—Inbound**
Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.)

Uncheck the check box to exclude the Redirecting Number IE.

You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.

**Enable Inbound FastStart**
Check this check box to enable the H.323 FastStart call connections on incoming calls.

By default, the check box remains unchecked for the H.323 gateway.

For intercluster calls, you must check the Enable Inbound FastStart check box on Cisco Unified Communications Manager servers in other clusters for the outbound FastStart feature to work.

**Note** If you updated Cisco Communications Manager 3.3(2) servers in other clusters with support patch B, do not enable inbound FastStart because 3.3(2)spB does not support the inbound FastStart feature over intercluster trunks.

**Call Routing Information - Outbound Calls**

**Calling Party Selection**
Any outbound call on a gateway can send directory number information. Choose which directory number is sent:

- **Originator**—Send the directory number of the calling device.
- **First Redirect Number**—Send the directory number of the redirecting device.
- **Last Redirect Number**—Send the directory number of the last device to redirect the call.
- **First Redirect Number (External)**—Send the directory number of the first redirecting device with the external phone mask applied.
- **Last Redirect Number (External)**—Send the directory number of the last redirecting device with the external phone mask applied.

**Calling Party Presentation**
Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number.

Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to send "Calling Line ID Allowed" on outbound calls. Choose Restricted if you want Cisco Unified Communications Manager to send "Calling Line ID Restricted" on outbound calls.

For more information about this field, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager System Guide*. 
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called party IE</td>
<td>Choose the format for the number type in called party directory numbers.</td>
</tr>
</tbody>
</table>
| Number Type Unknown   | Choose one of the following options:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type.  
• Unknown—This option specifies that 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.  |
| Calling party IE      | 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 type numbering plan.  |
| Number Type Unknown   | Choose one of the following options:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | • Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type.  
• Unknown—This option specifies that 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.  |
### Field: Called Numbering Plan

Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non-national type number.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—This option specifies that the dialing plan is unknown.

### Field: Calling Numbering Plan

Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—This option specifies that the dialing plan is unknown.
### Field | Description
--- | ---
**Caller ID DN** | Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America
- 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it.
- 5555000 = Fixed calling line ID. Use when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.
You can also enter the international escape character +.

**Display IE Delivery** | Check the check box to enable delivery of the display IE in SETUP, CONNECT, and NOTIFY messages for the calling and called party name delivery service.

**Redirecting Party Transformation CSS** | This setting allows you to transform the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of H.323 setup message sent out of Cisco Unified Communications Manager. Make sure that the Redirecting Party Transformation CSS that you choose contains either the calling or called party transformation pattern that you want to assign to this H.323 gateway.

**Note** If you configure the Redirecting Party Transformation CSS as None and also uncheck the Use Device Pool Redirecting Party CSS check box, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.

**Use Device Pool Redirecting Party CSS** | To use the Redirecting 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 Redirecting Party Transformation CSS that you configured in the H.323 Gateway Configuration window.

**Redirecting Number IE Delivery—Outbound** | Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified Communications Manager includes the Redirecting Number IE.)

Uncheck the check box to exclude the first redirecting number and the redirecting reason.

You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.

**Enable Outbound FastStart** | Check this check box to enable the H.323 FastStart feature on outgoing calls. By default, the check box remains unchecked for the H.323 gateway or trunk.

**Note** When you check the Enable Outbound FastStart check box, you must set the Media Termination Point Required, Media Resource Group Lists, and Codec for Outbound FastStart.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codec For Outbound FastStart</td>
<td>Use the drop-down list box to choose the codec for use with the H.323 device for an outbound FastStart call:</td>
</tr>
<tr>
<td></td>
<td>• G711 u-law 64K (default)</td>
</tr>
<tr>
<td></td>
<td>• G711 a-law 64K</td>
</tr>
<tr>
<td></td>
<td>• G723</td>
</tr>
<tr>
<td></td>
<td>• G729</td>
</tr>
<tr>
<td></td>
<td>• G729AnnexA</td>
</tr>
<tr>
<td></td>
<td>• G729AnnexB</td>
</tr>
<tr>
<td></td>
<td>• G729AnnexA-AnnexB</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When you check the Enable Outbound FastStart check box, you must choose the codec for supporting outbound FastStart calls. You may need to click Save prior to choosing the Codec For Outbound FastStart.</td>
</tr>
<tr>
<td>Use Device Pool Called Party Transformation CSS</td>
<td>To use the Called 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 Called Party Transformation CSS that you configured in the H.323 Gateway Configuration window.</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 H.323 Gateway Configuration window.</td>
</tr>
<tr>
<td>Geolocation Configuration</td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td>From the drop-down list box, choose a geolocation.</td>
</tr>
<tr>
<td></td>
<td>You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.</td>
</tr>
<tr>
<td></td>
<td>You can also choose a geolocation that has been configured with the <strong>System &gt; Geolocation Configuration</strong> menu option.</td>
</tr>
<tr>
<td></td>
<td>For an explanation of geolocations, including configuration details, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>For an overview and details of how logical partitioning uses geolocations, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>
From the drop-down list box, choose a geolocation filter. If you leave the `<None>` setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the **System > Geolocation Filter** menu option.

For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geolocation Filter</td>
<td>From the drop-down list box, choose a geolocation filter.</td>
</tr>
<tr>
<td></td>
<td>If you leave the <code>&lt;None&gt;</code> setting, no geolocation filter gets applied for this device.</td>
</tr>
<tr>
<td></td>
<td>You can also choose a geolocation filter that has been configured with the <strong>System &gt; Geolocation Filter</strong> menu option.</td>
</tr>
<tr>
<td></td>
<td>For an explanation of geolocation filters, including configuration details, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>For an overview and details of how logical partitioning uses geolocation filters, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>

### Incoming Calling Party Settings

<table>
<thead>
<tr>
<th>Field</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 Clear Prefix Settings.</td>
</tr>
<tr>
<td>Default Prefix Setting</td>
<td>To enter the default value for all prefix fields at the same time, click Default Prefix Settings.</td>
</tr>
</tbody>
</table>
Configure the following settings to globalize calling party numbers that use National 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 National for the Calling Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.
  
  If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of National type before it applies the prefixes.

- **Use Device Pool CSS**—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.

- **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.

  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.

**Tip** For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager Features and Services Guide*.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>- <strong>Prefix</strong>—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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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>Strip Digits</strong>—Enter the number of digits, up to the number 24, 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>- <strong>Use Device Pool CSS</strong>—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>- <strong>Calling Search Space</strong>—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. 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>
<tr>
<td></td>
<td><strong>Tip</strong> For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>
Configure the following settings to globalize calling party numbers that use International 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 International for the Calling Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.

  If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes.

- **Use Device Pool CSS**—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.

- **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.

  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.

**Tip** For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager Features and Services Guide*. 

<table>
<thead>
<tr>
<th>Field</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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes. • Use Device Pool CSS—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. • 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. 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>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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>• 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. 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. For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td></td>
<td>Tip</td>
</tr>
</tbody>
</table>
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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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**—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. 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.

  **Tip** For more information on configuring these settings, see topics related to Calling Search Space configuration settings in the *Cisco Unified Communications Manager Features and Services Guide*.

### Incoming Called Party Settings

The H.323 protocol does not support the international escape character +. To ensure the correct prefixes, including the +, get applied to inbound calls over H.323 gateways, configure the incoming called party settings; that is, configuring the incoming called party settings ensures that when an inbound call comes from a H.323 gateway, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the gateway.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Prefix Settings</td>
<td>To delete all prefixes for all called party number types, click Clear Prefix Settings.</td>
</tr>
<tr>
<td>Default Prefix Settings</td>
<td>To enter the default value for all prefix fields at the same time, click Default Prefix Settings.</td>
</tr>
</tbody>
</table>
Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Number</td>
<td>Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type.</td>
</tr>
<tr>
<td>Prefix</td>
<td>- Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. <strong>Tip</strong> If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. <strong>Tip</strong> To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field.</td>
</tr>
<tr>
<td>Strip Digits</td>
<td>- Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of National type before it applies the prefixes.</td>
</tr>
<tr>
<td>Use Device Pool CSS</td>
<td>- 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>Calling Search Space</td>
<td>- This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.</td>
</tr>
</tbody>
</table>
Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called 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 called party number of International type before it applies the prefixes.

- **Use Device Pool CSS**—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.

- **Calling Search Space**—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Number</td>
<td>Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type.</td>
</tr>
<tr>
<td>• Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong> If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality.</td>
<td></td>
</tr>
<tr>
<td>• Strip Digits—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes.</td>
<td></td>
</tr>
<tr>
<td>• Use Device Pool CSS—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>
<td></td>
</tr>
<tr>
<td>• Calling Search Space—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unknown Number</td>
<td>Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type.</td>
</tr>
<tr>
<td>• Prefix</td>
<td>Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 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><strong>Tip</strong></td>
<td>If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality.</td>
</tr>
<tr>
<td>• Strip Digits</td>
<td>Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>To configure the Strip Digits field, 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>• Use Device Pool CSS</td>
<td>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>• Calling Search Space</td>
<td>This setting allows you to transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.</td>
</tr>
</tbody>
</table>
Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type.

**Field** | **Description**
--- | ---
Subscriber Number | Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality.

**Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field.

- **Strip Digits**—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Subscriber type before it applies the prefixes.

- **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 transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

**Related Topics**

- Service parameter setup, on page 131
- About calling search space setup, on page 247
- Gateway setup, on page 433

**Analog access gateway settings**

The following table lists configuration settings for Analog Access gateways (Cisco Catalyst 6000 24 port FXS Gateway).
Table 77: Analog access gateway configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Information              | **MAC Address**
> Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device.
> You must enter a 12-hexadecimal character value.                                                                                                                                                      |
|                                 | **Description**
> Enter the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). |
|                                 | **Device Pool**
> From the drop-down list box, choose the appropriate device pool.
> The device pool specifies a collection of properties for this device including Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices. |
|                                 | **Common Device Configuration**
> From the drop-down list box, choose the common device configuration you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings. |
|                                 | **Media Resource Group List**
> This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines. |
|                                 | **Calling Search Space**
> From the drop-down list box, choose the appropriate calling search space. The calling search space specifies a collection of partitions that are searched to determine how a collected (originating) number should be routed.
> You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name.
> **Note**
> To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAadmin Parameters. |
|                                 | **AAR Calling Search Space**
> Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. |
**Field** | **Description**
--- | ---
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 device.  
A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.  
To configure a new location, use the **System > Location** menu option.  
For more details about locations, see the *Cisco Unified Communications Manager System Guide*.  

AAR Group | Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.  

Network Locale | From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area.  
**Note** Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
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:

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.
- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

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 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 Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:  
  - Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.  
  - Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  - On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  
  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 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 Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points. |
| Port Selection Order   | Choose the order in which ports are chosen. If you are not sure which port order to use, choose Top Down:  
  - Top Down—Selects ports in descending order, from port 1 to port 8.  
  - Bottom Up—Selects ports in ascending order, from port 8 to port 1. |
| Load Information       | Enter the appropriate firmware load information for the gateway.  
  The value that you enter here overrides the default firmware load for this gateway type. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit UTF-8 for Calling Party Name</td>
<td>This device uses the user locale setting of the device pool of the device to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device pool of the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the device pool of the sending device. If the user locale setting matches the terminating phone user locale, the phone displays the characters. <strong>Note</strong> The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.</td>
</tr>
<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. <strong>Tip</strong> 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 Gateway Configuration window.</td>
</tr>
<tr>
<td>MLPP Domain</td>
<td>From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value &lt;None&gt;, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
<tr>
<td>MLPP Indication</td>
<td>This device type does not have this setting.</td>
</tr>
<tr>
<td>MLPP Preemption</td>
<td>This setting does not have this device type.</td>
</tr>
<tr>
<td>Product-Specific Configuration</td>
<td></td>
</tr>
<tr>
<td>Model-specific configuration fields that the gateway manufacturer defines</td>
<td>The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.</td>
</tr>
</tbody>
</table>
**Geolocation Configuration**

From the drop-down list box, choose a geolocation.

You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.

You can also choose a geolocation that has been configured with the System > Geolocation Configuration menu option.

For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.

**Geolocation Filter**

From the drop-down list box, choose a geolocation filter.

If you leave the <None> setting, no geolocation filter gets applied for this device.

You can also choose a geolocation filter that has been configured with the System > Geolocation Filter menu option.

For an explanation of geolocation filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For an overview and details of how logical partitioning uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.

**Related Topics**

- About calling search space setup, on page 247
- Gateway setup, on page 433

**Cisco VG248 gateway settings**

The following table lists configuration settings for the Cisco VG248 Gateways.
Table 78: Cisco VG248 Gateway configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address (Last 10 Characters)</td>
<td>Enter the last 10 digits of the Media Access Control (MAC) address for the Cisco VG248. Only one MAC address exists for the Cisco VG248 Analog Phone Gateway, but Cisco Unified Communications Manager requires unique MAC addresses for all devices. When only 10 digits of the MAC address are entered, Cisco Unified Communications Manager can use the MAC address for the gateway and append additional information to it to create the MAC addresses for the VGC phones. The conversion of the MAC address for each device occurs by adding the two-digit port number to the end of the MAC address (to the right of the number) and adding VGC at the beginning of the MAC address. EXAMPLE MAC Address for the Cisco VG248 is 0039A44218 the MAC address for registered port 12 in Cisco Unified Communications Manager is VGC0039A4421812</td>
</tr>
<tr>
<td>Description</td>
<td>Cisco Unified Communications Manager automatically provides this information by adding VGCGW immediately in front of the MAC address.</td>
</tr>
<tr>
<td>Load Information</td>
<td>Enter the firmware version for the Cisco VG248 that is being configured; otherwise, leave blank to use the default.</td>
</tr>
<tr>
<td>Configured Slots, VICs and Endpoints</td>
<td>To begin configuring ports on a module, select the module first; then, click Save.</td>
</tr>
<tr>
<td>Note</td>
<td>From the list of endpoint identifiers, choose one of the ports to configure the VGC_Phone ports.</td>
</tr>
</tbody>
</table>

Related Topics

Gateway setup, on page 433

Cisco IOS SCCP gateway settings

The following table lists configuration settings for the Cisco IOS SCCP gateways.
Table 79: Cisco IOS SCCP gateway configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address (last 10 Characters)</td>
<td>Enter the last 10 digits of the Media Access Control (MAC) address for the gateway. Use the MAC address of the interface that the sccp local IOS command specifies on the gateway. Valid characters include the digits 0 through 9 and the uppercase characters A through F. The conversion of the MAC address for each device occurs by adding the three-digit mapping of the slot/subunit/port to the end of the MAC address (to the right of the number). EXAMPLE: MAC Address for the gateway is 0006D7E5C7. The MAC address in Cisco Unified Communications Manager is 0006D7E5C7281 where 281 is the three-digit mapping of the slot/subunit/port. The values 2, 8 and 1 can be hex digits and each do not necessarily correspond to slot, subunit and port values. The system inserts the following two-character strings before the MAC address to indicate the phone device types: • BR—BRI phone • AN—Analog phone The system also inserts SKIGW for the gateway name.</td>
</tr>
<tr>
<td>Description</td>
<td>Cisco Unified Communications Manager automatically provides this information by adding SKIGW immediately in front of the MAC address. You can override the description.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Group</td>
<td>From the drop-down list box, choose a Cisco Unified Communications Manager redundancy group. A Cisco Unified Communications Manager redundancy group includes a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager. If the primary Cisco Unified Communications Manager is not available or fails, the gateway attempts to connect with the next Cisco Unified Communications Manager in the list, and so on.</td>
</tr>
<tr>
<td>Configured Slots, VICS and Endpoints</td>
<td><strong>Note</strong> You must specify the beginning port number for some VICs. For example, if the VIC in Subunit 0 begins at 0 and has two ports (0 and 1), then the VIC in Subunit 1 must begin at a port number greater than 1 and have two ports (2 and 3 or 4 and 5). <strong>Note</strong> The correct number of slots displays for each model of SCCP gateway. <strong>Note</strong> To begin configuring ports on a module, select the module first; then, click Save.</td>
</tr>
</tbody>
</table>
For each available slot on the chosen SCCP gateway, choose the type of module that is installed. The system supports the following modules:

### Network Modules (with VIC slots):
- **NM-2V**—Has two VICs, one in Subunit 0 and one in Subunit 1 for FXS-SCCP.
- **NM-HD-2V**—Has two VIC slots, one in Subunit 0 and one in Subunit 1 for FXS-SCCP or for BRI-NT/TE-SCCP.
- **NM-HD-2VE**—Has two VIC slots, one in Subunit 0 and one in Subunit 1 for FXS-SCCP or for BRI-NT/TE-SCCP.

### Network Modules (no VIC slots):
- **NM-HDA-4FXS**—Has 4 FXS directly without VIC and can be extended by up to two expansion modules EM-HDA-8FXS to support 16 FXS ports.
- **EM-HDA-8FXS**—Expansion module for the NM-HDA-4FXS

### Voice Interface Cards:
- **VIC-2FXS**
- **VIC-4FXS**
- **VIC2-2FXS**
- **VIC2-2BRI-NT/TE**

At the slot level, these options exist:
- **NM-2V**—Two subunits with option VIC-2FXS-SCCP
- **NM-HD-2V**—Two subunits with options VIC-4FXS-SCCP, VIC2-2FXS-SCCP, VIC2-2BRI-NT/TE-SCCP
- **NM-HD-2VE**—Two subunits with options VIC-4FXS-SCCP, VIC2-2FXS-SCCP, VIC2-2BRI-NT/TE-SCCP
- **NM-HDA**—Three subunits with options NM-HDA-4FXS-SCCP, EM-8FXS-EM0-SCCP, EM-8FXS-EM1-SCCP
  - In NM-HDA, these options do not represent true VICs. The VIC2-2BRI-NT/TE represents the only VIC for BRI phones that are running SCCP. VG224 GW differs from all others.

The following option supports only one slot:
- **ANALOG**—One subunit option 24FXS-SCCP (supports 24 FXS ports)

The option None means that no network modules are installed.
The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice.

To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box.

If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Related Topics

Gateway setup, on page 433

Port setup

Tables that list detailed descriptions for all port type configuration fields are provided.

Related Topics

- FXS/FXO port settings, on page 467
- Digital access PRI port settings, on page 475
- Digital access T1 port settings, on page 495
- BRI port settings, on page 502
- POTS port settings, on page 515
- Loop-start port settings, on page 517
- Ground-start port settings, on page 518
- E and M port settings, on page 519

**FXS/FXO port settings**

The following table provides detailed descriptions for FXS/FXO port configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

For the VG200 gateway, not all switch emulation types support the network side. How you configure the gateway switch type determines whether you may or may not be able to set network side.

**Table 80: FXS/FXO port configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Cisco Unified Communications Manager generates a string that uniquely identifies the analog MGCP description. For example: AALN/S0/SU1/1@domain.com You can edit this field.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date and Time Group, Region, and Calling Search Space for auto registration of devices.</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that is defined in a Media Resource Group List.</td>
</tr>
<tr>
<td>Packet Capture Mode (for Cisco IOS MGCP gateways only)</td>
<td>Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Packet Capture Duration (for Cisco IOS MGCP gateways only)</td>
<td>Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the appropriate calling search space. A calling search space comprises a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. Note: To set the maximum list box items, choose System &gt; Enterprise Parameters and enter a value for Max List Box Items in the CCMAdmin Parameters pane.</td>
</tr>
<tr>
<td>AAR Calling Search Space</td>
<td>Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.</td>
</tr>
</tbody>
</table>
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 device.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the **System > Location** menu option.

For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area.

Choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.

<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 device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the <strong>System &gt; Location</strong> menu option. For an explanation of location-based CAC across intercluster trunks, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>AAR Group</td>
<td>Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.</td>
</tr>
<tr>
<td>Network Locale</td>
<td>From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area. <strong>Note</strong>: Choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Trusted Relay</td>
<td>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:&lt;br&gt;&lt;br&gt;• Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.&lt;br&gt;• Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.&lt;br&gt;• On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
<tr>
<td>Point</td>
<td>A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.&lt;br&gt;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).&lt;br&gt;If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the Cisco Unified Communications Manager System Guide for details of call behavior.&lt;br&gt;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.&lt;br&gt;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.&lt;br&gt;See the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.</td>
</tr>
<tr>
<td>Geolocation</td>
<td>From the drop-down list box, choose a geolocation.&lt;br&gt;You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.&lt;br&gt;You can also choose a geolocation that has been configured with the System &gt; Geolocation Configuration menu option.&lt;br&gt;For an explanation of geolocations, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide.&lt;br&gt;For an overview and details of how logical partitioning uses geolocations, see the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Transmit UTF-8 for Calling Party Name</td>
<td>This device uses the user locale setting of the device pool for the device to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device pool for the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool for the device. If the user locale setting matches the terminating phone user locale, the phone displays the characters. <strong>Note</strong> The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.</td>
</tr>
<tr>
<td>Enable Caller ID (for FXS ports)</td>
<td>To enable caller ID on this port, check this check box. Caller ID enables the port to report caller ID information, which can display on the destination phone when an incoming call arrives.</td>
</tr>
<tr>
<td>Ring Number (for FXS ports)</td>
<td>Enter the number of rings after which the port will answer an incoming call. The valid values are 1 or 2 rings. The default value is 1 ring.</td>
</tr>
<tr>
<td>Timing Guard-out</td>
<td>Enter the timing guard-out value, in milliseconds. This setting is a time window after a call is disconnected that no outgoing call is allowed. The range of valid values is 300 ms to 3000 ms. The default value is 1000 ms. Caller ID support requires a value of 1000 ms or less.</td>
</tr>
<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. <strong>Tip</strong> 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 Gateway Configuration window. This settings displays for FXS ports, not FXO ports.</td>
</tr>
<tr>
<td>Multilevel Precedence and Preemption (MLPP) Information</td>
<td>From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value '&lt;None&gt;', this device inherits its MLPP domain from the value set for the device pool for the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| MLPP Indication       | Be aware that this setting is not available for all devices. If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options:  
  - Default—This device inherits its MLPP indication setting from its device pool.  
  - Off—This device does not handle nor process indication of an MLPP precedence call.  
  - On—This device does handle and process indication of an MLPP precedence call. |
| Note                  | Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. |
| MLPP Preemption       | Be aware that this setting is not available for all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options:  
  - Default—This device inherits its MLPP preemption setting from its device pool.  
  - Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.  
  - Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. |
| Note                  | Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. |
| Port Information (POTS) |                                                                                                                                               |
| Port Direction        | Choose the direction of calls that are passing through this port:  
  - Inbound—Use for incoming calls only.  
  - Outbound—Use for outgoing calls.  
  - Bothways—Use for inbound and outbound calls (default). |
| Prefix DN (for FXS ports) | Enter the prefix digits that are appended to the digits that this trunk receives on incoming calls.  
Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Num Digits setting.  
You can enter the international escape character +. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num Digits(for FXS ports)</td>
<td>Enter the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number called. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that is used to route calls coming into the PRI span. See Prefix DN.</td>
</tr>
<tr>
<td>Expected Digits(for FXS ports)</td>
<td>Enter the number of digits that are expected on the inbound side of the trunk. For this rarely used field, leave zero as the default value if you are unsure.</td>
</tr>
<tr>
<td>SMDI Port Number (0-4096)</td>
<td>Use this field for analog access ports that connect to a voice-messaging system. Set the SMDI Port Number equal to the actual port number on the voice-messaging system to which the analog access port connects. <strong>Note</strong> Voice-mail logical ports typically must match physical ports for the voice-messaging system to operate correctly.</td>
</tr>
<tr>
<td>Unattended Port</td>
<td>Check this check box to indicate an unattended port on this device.</td>
</tr>
<tr>
<td>Product-Specific Configuration</td>
<td></td>
</tr>
<tr>
<td>Model-specific configuration fields defined by the gateway manufacturer</td>
<td>The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.</td>
</tr>
<tr>
<td>Geolocation Configuration</td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td>From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the System &gt; Geolocation Configuration menu option. For an explanation of geolocations, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide. For an overview and details of how logical partitioning uses geolocations, see the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
</tbody>
</table>
From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the System > Geolocation Filter menu option. For an explanation of geolocation filters, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide. For an overview and details of how logical partitioning uses geolocation filters, see the Cisco Unified Communications Manager Features and Services Guide.

Incoming Calling Party Settings

Clear Prefix Settings | To delete all prefixes for all calling party number types, click Clear Prefix Settings.

Default Prefix Settings | To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Strip Digits | Enter the number of preceding calling party number digits to remove. This value can also get configured by the device's device pool setting or the service parameter Incoming Calling Party Unknown Number Prefix – MGCP, depending on the port’s Prefix setting. To configure the service parameter Incoming Calling Party Unknown Number Prefix – MGCP to strip digits, enter a value in the format prefix:stripdigits, where prefix is the digits to prepend and stripdigits is the number of digits to strip.

Prefix | Enter the digits to prepend to the stripped calling party number. If you enter Default, the Strip Digits and Prefix settings get configured by the device pool Prefix setting. If the device pool Prefix setting is also set to Default, the Strip Digits and Prefix settings get configured by the service parameter Incoming Calling Party Unknown Number Prefix – MGCP.

Calling Search Space | Select a calling search space (CSS) from the drop-down list box that gets used to perform calling party number transformation. This setting can get overridden by the Use Devices Pool CSS field.

Use Device Pool CSS | Check this check box to use the device pool Unknown Number CSS to perform calling party number transformation. If this box is unchecked, the setting in the Calling Search Space field gets used.

Related Topics

Location setup, on page 107
About calling search space setup, on page 247
Gateway setup, on page 433
Digital access PRI port settings

The following table provides detailed descriptions for Digital Access PRI port configuration settings.

Table 81: Digital access PRI port configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td></td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>For MGCP gateways, this display-only field contains a string that is generated by Cisco Unified Communications Manager that uniquely identifies the MGCP endpoint. For example: S1/DS1-0@VG200-2 S1 indicates slot 1, DS1-0 designates the digital interface, and @VG200-2 designates the MGCP domain name.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device. You must enter a 12-hexadecimal character value.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Device Pool</td>
<td>From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>From the drop-down list box, choose the common device configuration you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.</td>
</tr>
<tr>
<td>Call Classification</td>
<td>This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Network Locale | From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that are used by the device in a specific geographic area.  
**Note** Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up. |
| Packet Capture Mode (for Cisco IOS MGCP gateways only) | Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide*. |
| Packet Capture Duration (for Cisco IOS MGCP gateways only) | Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the *Cisco Unified Communications Manager Security Guide*. |
| Media Resource Group List | This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, among the available media resources according to the priority order that is defined in a Media Resource List. |
| 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 device.  
A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.  
To configure a new location, use the System > Location menu option.  
For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*. |
| AAR Group | Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted. |
| Load Information | Enter the appropriate firmware load information for the gateway.  
The value that you enter here overrides the default firmware load for this gateway type. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Trusted Relay Point</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>• Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>• On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
<tr>
<td></td>
<td>A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.</td>
</tr>
<tr>
<td></td>
<td>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 RSVP Agent).</td>
</tr>
<tr>
<td></td>
<td>If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the Cisco Unified Communications Manager System Guide for details of call behavior.</td>
</tr>
<tr>
<td></td>
<td>If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVP Agent that can also be used as a TRP.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.</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>• Default—If you choose this value, the device uses the setting from the Route Class Signaling service parameter.</td>
</tr>
<tr>
<td></td>
<td>• Off—Choose this value to enable route class signaling. This setting overrides the Route Class Signaling service parameter.</td>
</tr>
<tr>
<td></td>
<td>• On—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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Transmit UTF-8 for Calling Party Name</td>
<td>This device uses the user locale setting of the device pool for the device to determine whether to send unicode and whether to translate received unicode information. For the sending device, if you check this check box and the user locale setting in the device pool for the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII. The receiving device translates incoming unicode characters based on the user locale setting of the device pool to which the sending device belongs. If the user locale setting matches the terminating phone user locale, the phone displays the characters. <strong>Note</strong> The phone may display junk characters if the two ends of the trunk configure user locales that do not belong to the same language group.</td>
</tr>
<tr>
<td>V150 (subset)</td>
<td>Check this box to enable V.150 (subset) modem relay support on the gateways. IP-STEs currently use this feature to support end-to-end secure calls to an ISDN-STE. (Applies only to T1 PRI and T1 CAS.) <strong>Note</strong> This setting supports both V.150 and V.150.1 MER (Minimal Essential Requirements) modem relay functionality. The default value specifies unchecked. <strong>Warning</strong> The MDSTE package must also be enabled on the gateway via a CLI command for this check box to work properly. If you check this box without enabling the gateway, the MDSTE package can cause call attempt failures on the affected gateway trunk.</td>
</tr>
</tbody>
</table>

### Multilevel Precedence and Preemption (MLPP) Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Domain</td>
<td>From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value &lt;None&gt;, this device inherits its MLPP domain from the value that is set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that is set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
</tbody>
</table>
| MLPP Indication | Be aware that this setting is not available for all devices. If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options:  
  - Default—This device inherits its MLPP indication setting from its device pool.  
  - Off—This device does not handle nor process indication of an MLPP precedence call.  
  - On—This device does handle and process indication of an MLPP precedence call. **Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| MLPP Preemption    | Be aware that this setting is not available for all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options:  
  • Default—This device inherits its MLPP preemption setting from its device pool.  
  • Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.  
  • Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.  

**Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Choose the communications protocol for the span.

T1 PRI spans provide several options, depending on the carrier or switch; for example:

- PRI 4ESS—AT&T Interexchange carrier
- PRI 5E8—AT&T family 5ESS ISDN switch that runs in NI-1 or custom mode.
- PRI 5E8 Custom—Cisco Unified IP Phone
- PRI 5E9—AT&T family local exchange switch or carrier
- PRI DMS—MCI family local exchange switch or carrier; Canadian local exchange carrier
- PRI ETSI SC—European local exchange carrier on T1; also, Japanese, Taiwan, Korean, and Hong Kong local exchange.
- PRI NI2—AT&T family local exchange switch or carrier

**Note** If you specify the PRI NI2 PRI protocol type, configure the Cisco IOS gateway with the following command:

```
isdn switch-type primary-ni
```

- PRI NTT—Japanese NTT exchange switch
- PRI ISO QSIG T1—PBX T1 tie trunk using ISO QSIG
- PRI ISO QSIG E1—PBX E1 tie trunk using ISO QSIG

Determine the switch to which you are connecting and the preferred protocol; for example:

- Nortel Meridian—DMS, 5E8 Custom
- Lucent Definity—4ESS or 5E8
- Madge (Teleos) box—5E8 Teleos
- Intecom PBX—5E8 Intecom

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRI Protocol Type</td>
<td>Choose the communications protocol for the span.</td>
</tr>
<tr>
<td></td>
<td>T1 PRI spans provide several options, depending on the carrier or switch; for example:</td>
</tr>
<tr>
<td></td>
<td>- PRI 4ESS—AT&amp;T Interexchange carrier</td>
</tr>
<tr>
<td></td>
<td>- PRI 5E8—AT&amp;T family 5ESS ISDN switch that runs in NI-1 or custom mode.</td>
</tr>
<tr>
<td></td>
<td>- PRI 5E8 Custom—Cisco Unified IP Phone</td>
</tr>
<tr>
<td></td>
<td>- PRI 5E9—AT&amp;T family local exchange switch or carrier</td>
</tr>
<tr>
<td></td>
<td>- PRI DMS—MCI family local exchange switch or carrier; Canadian local exchange carrier</td>
</tr>
<tr>
<td></td>
<td>- PRI ETSI SC—European local exchange carrier on T1; also, Japanese, Taiwan, Korean, and Hong Kong local exchange.</td>
</tr>
<tr>
<td></td>
<td>- PRI NI2—AT&amp;T family local exchange switch or carrier</td>
</tr>
</tbody>
</table>
| Note              | If you specify the PRI NI2 PRI protocol type, configure the Cisco IOS gateway with the following command:
isdn switch-type primary-ni |
<p>|                   | - PRI NTT—Japanese NTT exchange switch |
|                   | - PRI ISO QSIG T1—PBX T1 tie trunk using ISO QSIG |
|                   | - PRI ISO QSIG E1—PBX E1 tie trunk using ISO QSIG |
|                   | Determine the switch to which you are connecting and the preferred protocol; for example: |
|                   | - Nortel Meridian—DMS, 5E8 Custom |
|                   | - Lucent Definity—4ESS or 5E8 |
|                   | - Madge (Teleos) box—5E8 Teleos |
|                   | - Intecom PBX—5E8 Intecom |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QSIG Variant</td>
<td>To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, choose one of the following options. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise.</td>
</tr>
<tr>
<td></td>
<td>• No Changes</td>
</tr>
<tr>
<td></td>
<td>• Not Selected</td>
</tr>
<tr>
<td></td>
<td>• ECMA—If the QSIG Variant is set to ECMA (Protocol Profile 0x91), ensure the ASN.1 Rose OID Encoding service parameter is set to Use Global Value (ECMA).</td>
</tr>
<tr>
<td></td>
<td>• ISO—(Default) If the QSIG Variant is set to ISO (Protocol Profile 0x9F), ensure the ASN.1 Rose OID Encoding service parameter is set to either Use Local Value or Use Global Value (ISO).</td>
</tr>
<tr>
<td></td>
<td>For more information, see the following information:</td>
</tr>
<tr>
<td></td>
<td>• Be aware that the QSIG Variant can also be defined as a clusterwide parameter.</td>
</tr>
<tr>
<td></td>
<td>• For information on QSIG support with Cisco Unified Communications Manager, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>ASN.1 ROSE OID Encoding</td>
<td>To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• No Changes.</td>
</tr>
<tr>
<td></td>
<td>• Not Selected</td>
</tr>
<tr>
<td></td>
<td>• Use Global Value (ISO)—Select this option only if the connected PBX does not support Local Value.</td>
</tr>
<tr>
<td></td>
<td>• Use Global Value (ECMA)—Select this option only if the QSIG Variant service parameter is set to ECMA (Protocol Profile 0x91).</td>
</tr>
<tr>
<td></td>
<td>• Use Local Value—(Default) This option gets supported by most telephony systems and should be used when the QSIG Variant service parameter is set to ISO (Protocol Profile 0x9F).</td>
</tr>
<tr>
<td></td>
<td>For more information, see the following information:</td>
</tr>
<tr>
<td></td>
<td>• Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter.</td>
</tr>
<tr>
<td></td>
<td>• For information on QSIG support with Cisco Unified Communications Manager, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol Side</td>
<td>Choose the appropriate protocol side. This setting specifies whether the gateway connects to a Central Office/Network device or to a User device. Make sure that the two ends of the PRI connection use opposite settings. For example, if you connect to a PBX and the PBX uses User as its protocol side, choose Network for this device. Typically, use User for this option for central office connections.</td>
</tr>
<tr>
<td>Channel Selection Order</td>
<td>Choose the order in which channels or ports are enabled from first (lowest number port) to last (highest number port), or from last to first. Valid entries include TOP_DOWN (first to last) or BOTTOM_UP (last to first). If you are not sure which port order to use, choose TOP_DOWN.</td>
</tr>
<tr>
<td>Channel IE Type</td>
<td>Choose one of the following values to specify whether channel selection is presented as a channel map or a slot map:</td>
</tr>
<tr>
<td></td>
<td>• Timeslot Number—B-channel usage always indicates actual timeslot map format (such as 1-15 and 17-31 for E1).</td>
</tr>
<tr>
<td></td>
<td>• Slotmap—B-channel usage always indicates a slot map format.</td>
</tr>
<tr>
<td></td>
<td>• Use Number When 1B—Channel usage indicates a channel map for one B-channel but indicates a slot map if more than one B-channel exists.</td>
</tr>
<tr>
<td></td>
<td>• Continuous Number—Configures a continuous range of slot numbers (1-30) as the E1 logical channel number instead of the noncontinuous actual timeslot number (1-15 and 17-31).</td>
</tr>
<tr>
<td>PCM Type</td>
<td>Specify the digital encoding format. Choose one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• a-law: Use for Europe and other countries, except North America, Hong Kong, Taiwan, and Japan.</td>
</tr>
<tr>
<td></td>
<td>• mu-law: Use for North America, Hong Kong, Taiwan, and Japan.</td>
</tr>
<tr>
<td>Delay for first restart</td>
<td>Enter the rate at which the spans are brought in service. The delay occurs when many PRI spans are enabled on a system and the Inhibit Restarts at PRI Initialization check box is unchecked. For example, set the first five cards to 0 and set the next five cards to 16. (Wait 2 seconds before bringing them in service.)</td>
</tr>
<tr>
<td>Delay between restarts</td>
<td>Enter the time between restarts. The delay occurs when a PRI RESTART gets sent if the Inhibit Restarts check box is unchecked.</td>
</tr>
<tr>
<td>Inhibit restarts at</td>
<td>A RESTART or SERVICE message confirms the status of the ports on a PRI span. If RESTART or SERVICE messages are not sent, Cisco Unified Communications Manager assumes the ports are in service. When the D-Channel successfully connects with another PRI D-Channel, it sends a RESTART or SERVICE message when this check box is unchecked.</td>
</tr>
<tr>
<td>PRI initialization</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Enable status poll  | Check the check box to enable the Cisco Unified Communications Manager advanced service parameter, Change B-Channel Maintenance Status. This service parameter allows you to take individual B-channels out of service for an MGCP T1/E1 PRI gateway in real time.  
Uncheck this check box to disable the service parameter, Change B-Channel Maintenance Status.  
**Note** Default leaves this field unchecked. |
| Unattended Port     | Check this check box to indicate an unattended port on this device.                                                                                       |
| Enable G.Clear      | Check this box to enable G. Clear Codec support for MGCP T1 PRI gateways and SIP trunks. When you enable G. Clear Codec, echo cancellation and zero suppression for outbound calls get disabled.  
**Note** Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager Administration do not work.  
To enable G. Clear Code support on SIP trunks between clusters, you must configure the SIP Clear Channel Data Route Class Label and SIP Route Class Naming Authority service parameters.  
If you have low bandwidth codec regions, you must enable the G. Clear Bandwidth Override service parameter.  
The following functionality does not support the G. Clear Codec:  
• T1 and E1 CAS  
• H.323 Intercluster Trunks  
• SCCP devices  
• RSVP  
• Frame aligning individual DS-0 circuits |
| Significant Digits  | Choose the number of significant digits to collect, from 0 to 32 or All. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. If you choose All, the Cisco Unified Communications Manager does not truncate the inbound number.  
**EXAMPLE**Digits received are 123456.  
Significant digits setting is 4.  
Digits translated are 3456.  
Use for the processing of incoming calls and to indicate the number of digits, starting from the last digit of the called number, that are used to route calls that are coming into the PRI span. See Prefix DN. |
From the drop-down list box, choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed.

You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name.

**Note** To set the maximum list box items, choose System > Enterprise Parameters and choose CCMAdmin Parameters.

### Calling Search Space

Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.

### Prefix DN

Enter the prefix digits that are appended to the digits that this gateway receives on incoming calls.

The Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Num Digits setting.

You can enter the international escape character +.

### Call Routing Information - Outbound Calls

#### Calling Party Presentation

Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number.

Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to send "Calling Line ID Allowed" on outbound calls. Choose Restricted if you want Cisco Unified Communications Manager to send "Calling Line ID Restricted" on outbound calls.

For more information about this field, see the *Cisco Unified Communications Manager System Guide*.

#### Calling Party Selection

Any outbound call on a gateway can send directory number information. Choose which directory number is sent:

- **Originator**—Send the directory number of the calling device.
- **First Redirect Number**—Send the directory number of the redirecting device.
- **Last Redirect Number**—Send the directory number of the last device to redirect the call.
- **First Redirect Number (External)**—Send the directory number of the first redirecting device with the external phone mask applied.
- **Last Redirect Number (External)**—Send the directory number of the last redirecting device with the external phone mask applied.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called party IE</td>
<td>Choose the format for the number type in called party directory numbers.</td>
</tr>
<tr>
<td>number type unknown</td>
<td>Cisco Unified Communications Manager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NAP 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 called directory number to be encoded to a non-national type numbering plan. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Use when the dialing plan is unknown.</td>
</tr>
<tr>
<td></td>
<td>• National—Use when you are dialing within the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• International—Use when you are dialing outside the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.</td>
</tr>
<tr>
<td>Calling party IE</td>
<td>Choose the format for the number type in calling party directory numbers.</td>
</tr>
<tr>
<td>number type unknown</td>
<td>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 NAP 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 type numbering plan. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the directory number type.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Use when the dialing plan is unknown.</td>
</tr>
<tr>
<td></td>
<td>• National—Use when you are dialing within the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• International—Use when you are dialing outside the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Called Numbering Plan</td>
<td>Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.</td>
</tr>
<tr>
<td></td>
<td>• ISDN—Use when you are dialing outside the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• National Standard—Use when you are dialing within the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• Private—Use when you are dialing within a private network.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Use when the dialing plan is unknown.</td>
</tr>
<tr>
<td>Calling Numbering Plan</td>
<td>Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. 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 PBXs by using routing as a non-national type number. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager—Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.</td>
</tr>
<tr>
<td></td>
<td>• ISDN—Use when you are dialing outside the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• National Standard—Use when you are dialing within the dialing plan for your country.</td>
</tr>
<tr>
<td></td>
<td>• Private—Use when you are dialing within a private network.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Use when the dialing plan is unknown.</td>
</tr>
<tr>
<td>Number of digits to strip</td>
<td>Choose the number of digits to strip on outbound calls, from 0 to 32. For example, when 8889725551234 is dialed, and the number of digits to strip is 3, Cisco Unified Communications Manager strips 888 from the outbound number.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Caller ID DN** | Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America
- 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it.
- 5555000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.
You can also enter the international escape character +.

**SMDI Base Port** | Enter the first SMDI port number of the T1 span. If you set this parameter to a nonzero value and this gateway belongs to an unknown type of route list, route group, or route list, hunting does not continue past this span.

**Use Device Pool Called Party Transformation CSS** | To use the Called 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 Called Party Transformation CSS that you configured in the PRI Port Gateway Configuration window.

**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 PRI Port Gateway Configuration window.

**PRI Protocol Type Specific Information**

**Display IE Delivery** | Check the check box to enable delivery of the display information element (IE) in SETUP and NOTIFY messages (for DMS protocol) for the calling and connected party name delivery service.

**Redirecting Number IE Delivery—Outbound** | Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUID part of the outgoing SETUP message from the Cisco Unified Communications Manager includes the Redirecting Number IE.) Uncheck the box to exclude the first redirecting number and the redirecting reason. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirecting Party Transformation CSS</td>
<td>This setting allows you to transform the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of MGCP setup message sent out of Cisco Unified Communications Manager. Make sure that the Redirecting Party Transformation CSS that you choose contains either the calling or called party transformation pattern that you want to assign to this MGCP gateway. <strong>Note</strong> If you configure the Redirecting Party Transformation CSS as None and also uncheck the Use Device Pool Redirecting Party CSS check box, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.</td>
</tr>
<tr>
<td>Use Device Pool Redirecting Party CSS</td>
<td>To use the Redirecting 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 Redirecting Party Transformation CSS that you configured in the MGCP Gateway Configuration window.</td>
</tr>
<tr>
<td>Redirecting Number IE Delivery—Inbound</td>
<td>Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.) Uncheck the check box to exclude the Redirecting Number IE. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.</td>
</tr>
<tr>
<td>Send Extra Leading Character in Display IE</td>
<td>Check this check box to include a special leading character byte (non ASCII, nondisplayable) in the DisplayIE field. Uncheck this check box to exclude this character byte from the Display IE field. This check box only applies to the DMS-100 protocol and the DMS-250 protocol. Default leaves this setting disabled (unchecked).</td>
</tr>
<tr>
<td>Setup non-ISDN Progress Indicator IE Enable</td>
<td>Default leaves this setting disabled (unchecked). Enable this setting only if users are not receiving ringback tones on outbound calls. When this setting is enabled, the Cisco Unified Communications Manager sends Q.931 Setup messages out digital (that is, non-H.323) gateways with the Progress Indicator field set to non-ISDN. This message notifies the destination device that the Cisco Unified Communications Manager gateway is non-ISDN and that the destination device should play in-band ringback. This problem usually associates with Cisco Unified Communications Managers that connect to PBXs through digital gateways.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>MCDN Channel Number Extension Bit Set to Zero</td>
<td>To set the channel number extension bit to zero, check the check box. To set the extension bit to 1, uncheck the check box. This setting only applies to the DMS-100 protocol.</td>
</tr>
<tr>
<td>Send Calling Name in Facility IE</td>
<td>Check the check box to send the calling name in the Facility IE field. By default, the Cisco Unified Communications Manager leaves the check box unchecked. Set this feature for a private network that has a PRI interface that is enabled for ISDN calling name delivery. When this check box is checked, the calling party name gets sent in the Facility IE of the SETUP or FACILITY message, so the name can display on the called party device. Set this feature for PRI trunks in a private network only. Do not set this feature for PRI trunks that are connected to the PSTN. <strong>Note</strong> This field applies to the NI2 protocol only.</td>
</tr>
<tr>
<td>Interface Identifier Present</td>
<td>Check the check box to indicate that an interface identifier is present. By default, the Cisco Unified Communications Manager leaves the check box unchecked. This setting only applies to the DMS-100 protocol for digital access gateways in the Channel Identification information element (IE) of the SETUP, CALL PROCEEDING, ALERTING, and CONNECT messages.</td>
</tr>
<tr>
<td>Interface Identifier Value</td>
<td>Enter the value that was obtained from the PBX provider. This field applies to only the DMS-100 protocol. Valid values range from 0 through 255.</td>
</tr>
<tr>
<td>Connected Line ID Presentation (QSIG Inbound Call)</td>
<td>Choose whether you want the Cisco Unified Communications Manager to allow or block the connected party phone number from displaying on an inbound caller phone. This field applies only to gateways that are using QSIG protocol. The gateway applies this setting for incoming calls only. Choose Default if you do not want to change the connected line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to send “Connected Line ID Allowed” to enable the connected party number to display for the calling party. Choose Restricted if you want Cisco Unified Communications Manager to send “Connected Line ID Restricted” to block the connected party number from displaying for the calling party. If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed. For more information about this field, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>UUIE Configuration</td>
<td></td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing Precedence Level Through UUIE</td>
<td>Check this check box to enable passing MLPP information through the PRI 4ESS UUIE field. The system uses this box for interworking with DRSN switch. The system makes this check box available only if the PRI Protocol Type value of PRI 4ESS is specified for this gateway. The default value specifies unchecked.</td>
</tr>
<tr>
<td>Security Access Level</td>
<td>Enter the value for the security access level. Valid values include 00 through 99. The system makes this field available only if the Passing Precedence Level Through UUIE check box is checked. The default value specifies 2.</td>
</tr>
</tbody>
</table>

**Incoming Calling Party Settings**

| Clear Prefix Setting                            | To delete all prefixes for all calling party number types, click Clear Prefix Settings.                                                      |
| Default Prefix Setting                          | To enter the default value for all prefix fields at the same time, click Default Prefix Settings.                                           |
Configure the following settings to globalize calling party numbers that use National 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 National for the Calling Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of National type before it applies the prefixes.

- **Use Device Pool CSS**—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.

- **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. 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.

**Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>International</td>
<td>Configure the following settings to globalize calling party numbers that use International for the Calling Party Number Type.</td>
</tr>
<tr>
<td>Number</td>
<td></td>
</tr>
<tr>
<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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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>
<td></td>
</tr>
<tr>
<td>• Strip Digits—Enter the number of digits, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes.</td>
<td></td>
</tr>
<tr>
<td>• Use Device Pool CSS—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>
<td></td>
</tr>
<tr>
<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. 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>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>For more information on configuring these settings, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>
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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes.

- **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. 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.

**Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.  

<table>
<thead>
<tr>
<th>Field</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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Strip Digits—Enter the number of digits, up to the number 24, 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></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></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>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>
<tr>
<td></td>
<td>For more information on configuring these settings, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>


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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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**—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. 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.

**Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.  

### Product-Specific Configuration

The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box.

If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.
From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the System > Geolocation Configuration menu option.

For an explanation of geolocations, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide.

For an overview and details of how logical partitioning uses geolocations, see the Cisco Unified Communications Manager Features and Services Guide.

Geolocation Filter

From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the System > Geolocation Filter menu option.

For an explanation of geolocation filters, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide.

For an overview and details of how logical partitioning uses geolocation filters, see the Cisco Unified Communications Manager Features and Services Guide.

Related Topics

- Location setup, on page 107
- Service parameter setup, on page 131
- About calling search space setup, on page 247
- Gateway setup, on page 433

**Digital access T1 port settings**

The following table provides detailed descriptions for Digital Access T1 port configuration settings.

**Table 82: Digital access T1 port configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address (non-IOS gateway)</td>
<td>Enter MAC address of the gateway. The MAC address uniquely identifies the hardware device. You must enter a 12-hexadecimal character value.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain Name</td>
<td>For MGCP gateways, this display-only field contains a string that Cisco Unified Communications Manager generates that uniquely identifies the MGCP digital interface. For example S1/DS1-0@VG200-2. S1 indicates slot 1, DS1-0 designates the digital interface, and @VG200-2 designates the MGCP domain name.</td>
</tr>
<tr>
<td>Note</td>
<td>Enter either a MAC address or a domain name, whichever applies.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Device Pool</td>
<td>From the drop-down list box, choose the appropriate device pool. The device pool specifies a collection of properties for this device including Communications Manager Group, Date/Time Group, Region, and Calling Search Space for auto-registration of devices.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>From the drop-down list box, choose the common device configuration that you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.</td>
</tr>
<tr>
<td>Call Classification</td>
<td>This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that is defined in a Media Resource List.</td>
</tr>
<tr>
<td>Packet Capture Mode (for Cisco IOS MGCP gateways only)</td>
<td>Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Packet Capture Duration (for Cisco IOS MGCP gateways only)</td>
<td>Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed. You can configure the number of calling search spaces that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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, then find and choose a calling search space name. <strong>Note</strong> To set the maximum list box items, choose <strong>System &gt; Enterprise Parameters</strong> and choose CCMAdmin Parameters.</td>
</tr>
<tr>
<td>AAR Calling Search Space</td>
<td>Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.</td>
</tr>
<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 device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the <strong>System &gt; Location</strong> menu option. For more details about locations, see the <a href="#">Location setup, on page 107</a>. For an explanation of location-based CAC across intercluster trunks, see the <a href="#">Cisco Unified Communications Manager System Guide</a>.</td>
</tr>
<tr>
<td>AAR Group</td>
<td>Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.</td>
</tr>
<tr>
<td>MLPP Domain</td>
<td>From the drop-down list box, choose an MLPP domain to associate with this device. If you leave the value &lt;None&gt;, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| MLPP Indication     | Some devices do not make this setting available. If available, this setting specifies whether a device that plays precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options:  
  - Default—This device inherits its MLPP indication setting from its device pool.  
  - Off—This device does not handle nor process indication of an MLPP precedence call.  
  - On—This device does handle and process indication of an MLPP precedence call.  
  
  **Note**  
  Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. |
| MLPP Preemption     | Some devices do not make this setting available. If available, this 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 to assign to this device from the following options:  
  - Default—This device inherits its MLPP preemption setting from its device pool.  
  - Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.  
  - Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.  
  
  **Note**  
  Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable G. Clear Codec         | Check this box to enable G. Clear Codec support for MGCP T1 PRI gateways and SIP trunks. When you enable G. Clear Codec, echo cancellation and zero suppression for outbound calls get disabled. **Note** Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager Administration do not work. To enable G. Clear Code support on SIP trunks between clusters, you must configure the SIP Clear Channel Data Route Class Label and SIP Route Class Naming Authority service parameters. If you have low bandwidth codec regions, you must enable the G. Clear Bandwidth Override service parameter. The following functionality does not support the G. Clear Codec:  
  • T1 and E1 CAS  
  • H.323 Intercluster Trunks  
  • SCCP devices  
  • RSVP  
  • Frame aligning individual DS-0 circuits |
| Handle DTMF Precedence Signals| Check this box to enable this gateway to interpret special DTMF signals as MLPP precedence levels. |
| 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. |
| Load Information              | Enter the appropriate firmware load information for the gateway. The values that you enter here override the default values for this gateway. |
| Port Selection Order          | Choose the order in which channels or ports are allocated for outbound calls from first (lowest number port) to last (highest number port) or from last to first. Valid entries include Top Down (first to last) or Bottom Up (last to first). If you are not sure which port order to use, choose Top Down. |
| Digit Sending                 | Choose one of the following digit-sending types for out-dialing:  
  • DTMF—Dual-tone multifrequency. Normal touchtone dialing  
  • MF—Multifrequency  
  • PULSE—Pulse (rotary) dialing |
### Field | Description
--- | ---
Network Locale | From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area.
**Note** | Choose only a network locale that is already installed and supported by the associated devices. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up.
SMDI Base Port | Enter the first SMDI port number of the T1 span.
If you set this parameter to a nonzero value and this gateway belongs to an unknown type of route list, route group, or route list, hunting does not continue past this span.
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:

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.
- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.
- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

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 *Cisco Unified Communications Manager System Guide* for details of call behavior.
If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVP Agent 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 *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| V150 (subset)                 | Check this box to enable V.150 (subset) modem relay support on the gateways. IP-STEs currently use this feature to support end-to-end secure calls to an ISDN-STE. (Applies only to T1 PRI and T1 CAS)  
  **Note** This setting supports both V.150 and V.150.1 MER (Minimal Essential Requirements) modem relay functionality.  
  The default value specifies unchecked.                                                                                                                                                 |
| Product-Specific Configuration | The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice.  
  To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box.  
  If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.                                                        |
| Geolocation Configuration     | The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice.  
  To view field descriptions and help for product-specific configuration items, click the "?" information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box.  
  If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.                                                        |

For an explanation of geolocations, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide.

For an overview and details of how logical partitioning uses geolocations, see the Cisco Unified Communications Manager Features and Services Guide.
From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the System > Geolocation Filter menu option.

For an explanation of geolocation filters, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide.

For an overview and details of how logical partitioning uses geolocation filters, see the Cisco Unified Communications Manager Features and Services Guide.

### Related Topics

- About calling search space setup, on page 247
- Gateway setup, on page 433

### BRI port settings

The following table provides detailed descriptions for BRI port configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Information</strong></td>
<td></td>
</tr>
<tr>
<td>End-Point Name (MGCP gateways)</td>
<td>For MGCP gateways, this display-only field contains a string that Cisco Unified Communications Manager generates that uniquely identifies the MGCP endpoint. For example BRI/S1/SU0/P0@SC3640.cisco.com S1 indicates slot 1, SU0 indicates subunit 0, P0 indicates port 0, and @SC3640.cisco.com designates the MGCP domain name.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that clarifies the purpose of the device. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Device Pool</td>
<td>From the drop-down list box, choose the appropriate device pool. For this device, the device pool specifies a collection of properties that includes Communications Manager Group, Date and Time Group, Region, and Calling Search Space for auto-registration of devices.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>From the drop-down list box, choose the common device configuration you want to use for this gateway. The common device configuration determines softkey template, MOH, and MLPP settings.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call Classification</td>
<td>This parameter determines whether an incoming call that is using this gateway is considered off the network (OffNet) or on the network (OnNet). When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the gateway is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively.</td>
</tr>
<tr>
<td>Network Locale</td>
<td>From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that devises use in a specific geographic area.</td>
</tr>
<tr>
<td>Packet Capture Mode (for Cisco IOS MGCP gateways only)</td>
<td>Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Packet Capture Duration (for Cisco IOS MGCP gateways only)</td>
<td>Configure this field only when you need to troubleshoot encrypted signaling information for the Cisco IOS MGCP gateway. Configuring packet capturing may cause call-processing interruptions. For more information on this field, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource List defines.</td>
</tr>
<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 device. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this device consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the <strong>System &gt; Location</strong> menu option. For an explanation of location-based CAC across intercluster trunks, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
---|---
AAR Group | Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

**Interface Information**

**BRI Protocol** | Choose the communications protocol for the span. BRI-NET3

**Protocol Side** | Choose the appropriate protocol side. This setting specifies whether the gateway connects to a Central Office/Network device or to a User device. **Note** BRI supports only the User side.

**Channel Selection Order** | Choose the order in which channels or ports are enabled from first (lowest number port) to last (highest number port) or from last to first. Valid entries include TOP_DOWN (first to last) or BOTTOM_UP (last to first). If you are not sure which port order to use, choose TOP_DOWN.

**PCM Type** | Specify the digital encoding format. Choose one of the following formats:
- *a-law*: Use for Europe and other countries, except North America, Hong Kong, Taiwan, and Japan.
- *mu-law*: Use for North America, Hong Kong, Taiwan, and Japan.

**Delay for First Restart (1/8 sec ticks)** | Enter the rate at which the spans are brought in service. The delay occurs when many BRI spans are enabled on a system and the Inhibit Restarts at BRI Initialization check box is unchecked. For example, set the first five cards to 0 and set the next five cards to 16. (Wait 2 seconds before bringing them in service.)

**Delay Between Restarts (1/8 sec ticks)** | Enter the time between restarts. The delay occurs when a BRI RESTART gets sent if the Inhibit Restarts check box is unchecked.

**Inhibit Restarts at BRI Initialization** | A RESTART message confirms the status of the ports on a BRI span. If RESTART messages are not sent, Cisco Unified Communications Manager assumes that the ports are in service. When the data link successfully connects with another BRI data link, it sends a RESTART message when this check box is unchecked.

**Enable Status Poll** | Check the check box to view the B-channel status in the debug window.
### Field | Description
--- | ---
Enable G.Clear | Check this box to enable G. Clear Codec support for MGCP BRI gateways and SIP trunks. When you enable G. Clear Codec, echo cancellation and zero suppression for outbound calls get disabled.  
**Note** Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager Administration do not work.  
To enable G. Clear Code support on SIP trunks between clusters, you must configure the SIP Clear Channel Data Route Class Label and SIP Route Class Naming Authority service parameters.  
If you have low bandwidth codec regions, you must enable the G. Clear Bandwidth Override service parameter.  
The following functionality does not support the G. Clear Codec:  
• T1 and E1 CAS  
• H.323 Intercluster Trunks  
• SCCP devices  
• RSVP  
• Frame aligning individual DS-0 circuits

Establish Datalink on First Call | Cisco Unified Communications Manager establishes the data link to the gateway when the gateway registers with Cisco Unified Communications Manager.  
When you configure the gateway and switch to negotiate the TEI (terminal endpoint identifier) on the first call, you can check the check box to establish the data link on the first call.  
**Note** Default leaves the check box unchecked.

Call Routing Information - Inbound Calls |  
Significant Digits | Choose the number of significant digits to collect, from 0 to 32 or All. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number called. If you choose All, the Cisco Unified Communications Manager does not truncate the inbound number.  
**EXAMPLE** Digits received are 123456. Significant digits setting is 4. Digits translated are 3456.  
Use for the processing of incoming calls and to indicate the number of digits, starting from the last digit of the called number, that are used to route calls that are coming into the BRI span. See Prefix DN.  

Calling Search Space | Choose the appropriate calling search space. A calling search space designates a collection of route partitions that are searched to determine how a collected (originating) number should be routed.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR Calling Search Space</td>
<td>Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.</td>
</tr>
<tr>
<td>Prefix DN</td>
<td>Enter the prefix digits that are appended to the digits that this gateway receives on incoming calls. The Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Num Digits setting. You can enter the international escape character + in this field.</td>
</tr>
<tr>
<td>Call Routing Information - Outbound Calls</td>
<td></td>
</tr>
</tbody>
</table>
| Called Party Transformation CSS | This setting allows you to localize the called party number on the device. Make sure that the Called Party Transformation CSS that you choose contains the called party transformation pattern that you want to assign to this device.  
**Note** If you configure the Called Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Called Party Transformation pattern in a non-null partition that is not used for routing. |
| Use Device Pool Called Party Transformation CSS | To use the Called 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 Called Party Transformation CSS that you configured in the PRI Port Gateway Configuration window. |
| Calling Party Transformation CSS | This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.  
**Tip** 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. |
| Geolocation                   | From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.  
You can also choose a geolocation that has been configured with the **System > Geolocation Configuration** menu option.  
For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.  
For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 PRI Port Gateway Configuration window.</td>
</tr>
<tr>
<td>Calling Party Presentation</td>
<td>Choose whether you want the Cisco Unified Communications Manager to transmit or block caller ID. Choose Default if you do not want to change calling party presentation. Choose Allowed if you want Cisco Unified Communications Manager to send caller ID. Choose Restricted if you do not want Cisco Unified Communications Manager to send caller ID.</td>
</tr>
</tbody>
</table>
| Calling Party Selection                   | Any outbound call on a gateway can send directory number information. Choose which directory number is sent:  
  - Originator—Send the directory number of the calling device.  
  - First Redirect Number—Send the directory number of the redirecting device.  
  - Last Redirect Number—Send the directory number of the last device to redirect the call.  
  - First Redirecting Party (External)—Send the directory number of the first redirecting device with the external phone mask applied.  
  - Last Redirecting Party (External)—Send the directory number of the last redirecting device with the external phone mask applied. |
| Called party IE number type unknown       | Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national numbering plan type. Choose one of the following options:  
  - Communications Manager—The Cisco Unified Communications Manager sets the directory number type.  
  - International—Use when you are dialing outside the dialing plan for your country.  
  - National—Use when you are dialing within the dialing plan for your country.  
  - Unknown—The dialing plan is unknown.  
  - Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Calling party IE number type unknown | 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 NAP 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:  
  - Communications Manager—The Cisco Unified Communications Manager sets the directory number type.  
  - International—Use when you are dialing outside the dialing plan for your country.  
  - National—Use when you are dialing within the dialing plan for your country.  
  - Unknown—The dialing plan is unknown.  
  - Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number. |
| Called Numbering Plan       | Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NAP 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 PBXs by using routing as a non-national type number. Choose one of the following options:  
  - Communications Manager—The Cisco Unified Communications Manager sets the Numbering Plan in the directory number.  
  - ISDN—Use when you are dialing outside the dialing plan for your country.  
  - National Standard—Use when you are dialing within the dialing plan for your country.  
  - Private—Use when you are dialing within a private network.  
  - Unknown—The dialing plan is unknown.  
  - Subscriber—Use when you are dialing a subscriber by using a shortened subscriber number. |
### Field | Description
---|---
Calling Numbering Plan | Choose the format for the numbering plan in calling party directory numbers.
Cisco Unified Communications Manager sets the calling DN numbering plan.
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 PBXs by using routing as a non-national type number.

Choose one of the following options:

- **Communications Manager**—The Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—The dialing plan is unknown.
- **Subscriber**—Use when you are dialing a subscriber by using a shortened subscriber number.

Number of digits to strip | Choose the number of digits to strip on outbound calls, from 0 to 32.
For example, when 8889725551234 is dialed, and the number of digits to strip is 3, Cisco Unified Communications Manager strips 888 from the outbound number.

Caller ID DN | Enter the pattern that you want to use for caller ID, from 0 to 24 digits.
For example, in North America

- **555XXXX** = Variable caller ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it.
- **5555000** = Fixed caller ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.

You can also enter the international escape character `+`.

Incoming Calling Party Settings

Clear Prefix Setting | To delete all prefixes for all calling party number types, click Clear Prefix Settings.

Default Prefix Setting | To enter the default value for all prefix fields at the same time, click Default Prefix Settings.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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—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. 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>
<tr>
<td>Tip</td>
<td>For more information on configuring these settings, see topics related to location configuration in the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
</tbody>
</table>
Configure the following settings to globalize calling party numbers that use International 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 International for the Calling Party Number Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.

  If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes.

- **Use Device Pool CSS**—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.

- **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.

  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.

**Tip** For more information on configuring these settings, see topics related to location configuration in the *Cisco Unified Communications Manager Features and Services Guide*.
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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).

  If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes.

- **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 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.

  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.

**Tip** For more information on configuring these settings, see topics related to location configuration in the *Cisco Unified Communications Manager Features and Services Guide*.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).  
    If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes.  
  - 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 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.  
    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.  
  For more information on configuring these settings, see topics related to location configuration in the *Cisco Unified Communications Manager Features and Services Guide*. |
**Field** | **Description**  
--- | ---  
Unknown Number | 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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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**—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. 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.  

**Tip** For more information on configuring these settings, see topics related to configuring the incoming calling party settings for a device pool, gateway, or trunk in the *Cisco Unified Communications Manager Features and Services Guide*.  

BRI Protocol Type Specific Information
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirecting Number IE Delivery— Outbound</td>
<td>Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified Communications Manager includes the Redirecting Number IE.) Uncheck the check box to exclude the first redirecting number and the redirecting reason. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. <strong>Note</strong> Default leaves the check box checked.</td>
</tr>
<tr>
<td>Redirecting Party Transformation CSS</td>
<td>This setting allows you to transform the redirecting party number on the device to another format such as DID or E164 format. Cisco Unified Communications Manager includes the transformed number in the Redirecting Number Information Element of MGCP setup message sent out of Cisco Unified Communications Manager. Make sure that the Redirecting Party Transformation CSS that you choose contains either the calling or called party transformation pattern that you want to assign to this MGCP gateway. <strong>Note</strong> If you configure the Redirecting Party Transformation CSS as None and also uncheck the Use Device Pool Redirecting Party CSS check box, the transformation does not match and does not get applied. Ensure that you configure the Redirecting Party Transformation CSS in a non-null partition that is not used for routing.</td>
</tr>
<tr>
<td>Use Device Pool Redirecting Party Transformation CSS</td>
<td>To use the Redirecting 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 Redirecting Party Transformation CSS that you configured in the MGCP Gateway Configuration window.</td>
</tr>
<tr>
<td>Redirecting Number IE Delivery— Inbound</td>
<td>Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.) Uncheck the check box to exclude the Redirecting Number IE. You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box. <strong>Note</strong> Default leaves the check box checked.</td>
</tr>
</tbody>
</table>
Setup non-ISDN Progress Indicator IE Enable

Default leaves this setting disabled (unchecked).

Enable this setting only if users are not receiving ringback tones on outbound calls.

When this setting is enabled, the Cisco Unified Communications Manager sends Q.931 Setup messages out digital (that is, non-H.323) gateways with the Progress Indicator field set to non-ISDN.

This message notifies the destination device that the Cisco Unified Communications Manager gateway is non-ISDN and that the destination device should play in-band ringback.

This problem usually associates with Cisco Unified Communications Managers that connect to PBXs through digital gateways.

Product-Specific Configuration

Model-specific configuration fields that are defined by the gateway manufacturer

The model-specific fields under product-specific configuration define the gateway manufacturer. Because they are dynamically configured, they can change without notice.

To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box.

If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

Related Topics

Location setup, on page 107
Gateway setup, on page 433

POTS port settings

The following table describes the POTS port configuration settings.

Table 84: POTS port configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Selection</td>
<td></td>
</tr>
<tr>
<td>Port Type</td>
<td>For POTS ports, this field displays POTS.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Beginning Port Number</td>
<td>Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields:</td>
</tr>
<tr>
<td>Ending Port Number</td>
<td>• To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number.</td>
</tr>
<tr>
<td></td>
<td>• To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields.</td>
</tr>
<tr>
<td></td>
<td>• To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.</td>
</tr>
<tr>
<td>Port Details</td>
<td></td>
</tr>
<tr>
<td>Port Direction</td>
<td>Choose the direction of calls that pass through this port:</td>
</tr>
<tr>
<td></td>
<td>• Inbound—Use for incoming calls only.</td>
</tr>
<tr>
<td></td>
<td>• Outbound—Use for outgoing calls.</td>
</tr>
<tr>
<td></td>
<td>• Bothways—Use for inbound and outbound calls (default).</td>
</tr>
<tr>
<td>Audio Signal Adjustment into IP Network</td>
<td>This field specifies the gain or loss that is applied to the received audio signal relative to the port application type.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Improper gain setting may cause audio echo. Use caution when you are adjusting this setting.</td>
</tr>
<tr>
<td>Audio Signal Adjustment from IP Network</td>
<td>This field specifies the gain or loss that is applied to the transmitted audio signal relative to the port application type.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Improper gain setting may cause audio echo. Use caution when you are adjusting this setting.</td>
</tr>
<tr>
<td>Prefix DN</td>
<td>Enter the prefix digits that are appended to the digits that this gateway receives on incoming calls.</td>
</tr>
<tr>
<td></td>
<td>The Cisco Unified Communications Manager adds prefix digits after it truncates the number in accordance with the Num Digits setting.</td>
</tr>
<tr>
<td></td>
<td>You can enter the international escape character +.</td>
</tr>
<tr>
<td>Num Digits</td>
<td>Enter the number of significant digits to collect, from 0 to 32.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called.</td>
</tr>
<tr>
<td></td>
<td>Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that are used to route calls that are coming into the PRI span. See Prefix DN.</td>
</tr>
<tr>
<td>Expected Digits</td>
<td>Enter the number of digits that are expected on the inbound side of the trunk. For this rarely used field, leave zero as the default value if you are unsure.</td>
</tr>
</tbody>
</table>
Loop-start port settings

The following table describes the loop-start port configuration settings.

Table 85: Loop-start port configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>From the Port Type drop-down list box, choose Loop Start.</td>
</tr>
</tbody>
</table>
Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Port Number and End Port Number fields:

- To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number.
- To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields.
- To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.

Choose the direction of calls that pass through this port:

- Inbound—Use for incoming calls only.
- Outbound—Use for outgoing calls.
- Both Ways—Use for inbound and outbound calls.

Enter the directory number to which you want incoming calls routed; for example, zero or a directory number for an attendant.

Check this check box to indicate an unattended port on this device.

The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box.

If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

**Related Topics**

Gateway setup, on page 433

**Ground-start port settings**

The following table describes the ground-start port configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>From the Port Type drop-down list box, choose Ground Start.</td>
</tr>
</tbody>
</table>
Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields:

- To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number.
- To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields.
- To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.

Choose the direction of calls that pass through this port:

- Inbound—Use for incoming calls only.
- Outbound—Use for outgoing calls.
- Both Ways—Use for inbound and outbound calls.

Enter the number to which you want incoming calls to be routed; for example, zero or a directory number for an attendant.

Check this check box to indicate an unattended port on this device.

The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice.

To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box.

If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.

**Related Topics**

Gateway setup, on page 433

**E and M port settings**

E & M (Ear and Mouth) ports allow connection for PBX trunk lines (tie lines). E & M designates a signaling technique for two-wire, four-wire, and six-wire telephone and trunk interfaces.

The following table describes the E & M port configuration settings.
### Table 87: E & M port configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>From the Port Type drop-down list box, choose EANDM.</td>
</tr>
<tr>
<td>Beginning Port Number</td>
<td>Choose whether you want to add and configure all available ports, a single port, or a range of ports by setting values for the Beginning Port Number and Ending Port Number fields:</td>
</tr>
<tr>
<td>Ending Port Number</td>
<td>• To specify a range of ports, choose appropriate values for Beginning Port Number and Ending Port Number.</td>
</tr>
<tr>
<td></td>
<td>• To create a single port, choose the same number in the Beginning Port Number and Ending Port Number fields.</td>
</tr>
<tr>
<td></td>
<td>• To add all available ports, choose All Ports for both the Beginning Port Number and Ending Port Number fields.</td>
</tr>
</tbody>
</table>

#### Port Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Direction</td>
<td>Choose the direction of calls that pass through this port:</td>
</tr>
<tr>
<td></td>
<td>• Inbound—Use for incoming calls only.</td>
</tr>
<tr>
<td></td>
<td>• Outbound—Use for outgoing calls.</td>
</tr>
<tr>
<td></td>
<td>• Both Ways—Use for inbound and outbound calls.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Party Selection</td>
<td>Any outbound call on a gateway can send directory number information. Choose which directory number is sent:</td>
</tr>
<tr>
<td></td>
<td>• Originator—Send the directory number of the calling device.</td>
</tr>
<tr>
<td></td>
<td>• First Redirect Number—Send the directory number of the redirecting device.</td>
</tr>
<tr>
<td></td>
<td>• Last Redirect Number—Send the directory number of the last device to redirect the call.</td>
</tr>
<tr>
<td></td>
<td>• First Redirect Number (External)—Send the directory number of the first redirecting device with the external phone mask applied.</td>
</tr>
<tr>
<td></td>
<td>• Last Redirect Number (External)—Send the directory number of the last redirecting device with the external phone mask applied.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller ID Type</td>
<td>Choose the caller ID type:</td>
</tr>
<tr>
<td></td>
<td>• ANI—Choose this type to use the Asynchronous Network Interface (ANI) caller ID type.</td>
</tr>
<tr>
<td></td>
<td>• DNIS—Choose this type to use the Dialed Number Identification Service (DNIS) caller ID type.</td>
</tr>
</tbody>
</table>
**Field** | **Description**  
---|---  
Caller ID DN | Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America  
  - 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it.  
  - 5555000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.  
You can also enter the international escape character +.  
Prefix DN | Enter the prefix digits that are appended to the called party number on incoming calls. The Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Num Digits setting. You can enter the international escape character +.  
Num Digits | Choose the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. Use this field if you check the Sig Digits check box. Use this field for the processing of incoming calls and to indicate the number of digits starting from the last digit of the called number that are used to route calls that are coming into the PRI span. See Prefix DN and Sig Digits.  
Expected Digits | Enter the number of digits that are expected on the inbound side of the trunk. If you are unsure, leave zero as the default value for this rarely used field.  
Product-Specific Configuration  
Model-specific configuration fields that the gateway manufacturer defines | The gateway manufacturer specifies the model-specific fields under product-specific configuration. Because they are dynamically configured, they can change without notice. To view field descriptions and help for product-specific configuration items, click the “?” information icon to the right of the Product Specific Configuration heading to display help in a popup dialog box. If you need more information, see the documentation for the specific gateway that you are configuring or contact the manufacturer.  

**Related Topics**  
Gateway setup, on page 433
Add gateway to Cisco Unified Communications Manager

To enable Cisco Unified Communications Manager to manage IP telephony gateways in your network, you must first add each gateway to the Cisco Unified Communications Manager configuration database. The procedures, windows, and configuration settings for adding a gateway vary according to the gateway model that you are adding.

The following procedure describes how to add a new gateway in Cisco Unified Communications Manager.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>To display the Find and List Gateways window, choose <strong>Device &gt; Gateway</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the Add New button. The Add a New Gateway window displays.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the Gateway Type drop-down list box, choose the gateway type that you want to add. The Device Protocol field may automatically get populated depending on gateway type that you choose.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Next.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In Table 88: Gateways, on page 522, click the specific procedure for the gateway type that you are configuring. After you are in the correct procedure, start with the step where you enter the appropriate settings for that particular gateway type.</td>
</tr>
</tbody>
</table>

**Gateway addition associated procedures**

The following table lists the procedure to add a gateway for each type of gateway that is supported.

<table>
<thead>
<tr>
<th>Type of Gateway</th>
<th>Procedure to Add</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Voice Gateway 200 (VG200) VG224 Gateway Cisco IOS 269X, 26XX, 362X, 364X, 366X, 3725, 3745 Gateways Cisco 2801, 2811, 2821, 2851, 3825, 3845 Gateways Cisco Catalyst 4000 Access Gateway Module Cisco Catalyst 4224 Voice Gateway Switch Communication Media Module Cisco IAD2400 Cisco IOS 269X, 3725, 3745 Gateways</td>
<td>Use the procedure to add a Cisco IOS MGCP gateway. Use the procedure to add a Cisco IOS SCCP gateway.</td>
</tr>
</tbody>
</table>
Procedure to AddType of Gateway

Use the procedure to add a Non-IOS MGCP gateway.
Cisco Catalyst 6000 E1 VoIP Gateway
Cisco Catalyst 6000 T1 VoIP Gateway

Use the procedure to add a Cisco IOS H.323 gateway.
Other Cisco IOS Gateway that is configured in H.323 mode

Use the procedure to add an analog access gateway and ports.
Cisco Catalyst 6000 24 Port FXS Gateway

Use the procedure to add a Cisco VG248 analog phone gateway.
Cisco VG248 Gateway

Related Topics
Add Cisco IOS MGCP gateway, on page 523
Add Cisco IOS SCCP gateway, on page 529
Add non-IOS MGCP gateway, on page 530
Add Cisco IOS H.323 gateway, on page 531
Add analog access gateway and ports, on page 532
Add Cisco VG248 analog phone gateway, on page 532

Add Cisco IOS MGCP gateway

Use the following procedure to add and configure a Cisco IOS MGCP gateway to Cisco Unified Communications Manager. The following Cisco IOS gateways support MGCP:

- Cisco VG200 Voice Gateway
- VG224 Gateway
- Cisco IOS 362x, 364x, 366x Gateways
- Cisco IOS 3725 and 3745 Gateways
- Cisco IOS 26xx and 269x Gateways
- Cisco 2801, 2811, 2821, 2851, 3825, 3845 Gateways
- Cisco Catalyst 4000 Access Gateway Module
- Cisco Catalyst 4224 Voice Gateway Switch
- Communication Media Module
- Cisco IAD2400 gateways

Like other IOS MGCP gateways, MRP/ASI gateways may work with a Cisco Unified Communications Manager group that contains three Cisco Unified Communications Managers. ASI/MRP gateways testing occurs, however, with only one backup Cisco Unified Communications Manager.
Before You Begin

Before configuring a Cisco IOS MGCP gateway for use with Cisco Unified Communications Manager, you must configure the gateway by using the Cisco IOS command-line interface (CLI). For procedures and commands that are required to perform this configuration, see the configuration documentation that is supplied with the gateway.

Procedure

**Step 1**  
To display the Find and List Gateways window, choose **Device > Gateway**.

**Step 2**  
Click the Add New button. The Add a New Gateway window displays.

**Step 3**  
From the Gateway Type drop-down list box, choose one of the following MGCP gateways:

a) Cisco VG200  
b) VG224  
c) Cisco 362X, 364X, 366X  
d) Cisco 3725 and 3745  
e) Cisco 26XX and 269X  
f) Cisco 2801, 2811, 2821, 2851, 3825, 3845  
g) Cisco Catalyst 4000 Access Gateway Module  
h) Cisco Catalyst 4224 Voice Gateway Switch  
i) Communication Media Module  
j) Cisco IAD2400

**Note**  
The Cisco Catalyst 6000 gateways also support MGCP but are configured differently.

Cisco IOS MGCP gateways support different device protocols for interfacing to the PSTN or other non-IP devices, depending on the gateway model and the type of installed network modules and voice interface cards (VICs). A subsequent web window provides configuration for these interfaces.

**Step 4**  
Click Next.

**Step 5**  
If a Protocol drop-down list box displays, choose MGCP and click Next. Otherwise, skip to **Step 6**, on page 524.

**Step 6**  
The appropriate Gateway Configuration window displays. Enter the appropriate settings and choose the type of network modules that are installed in each slot, as described in the Table 75: MGCP gateway configuration settings, on page 435, including any product-specific configuration settings.

**Step 7**  
Click Save.  
The Gateway Configuration window updates and displays drop-down list boxes with options for configuring the type of voice interface cards (VICs) in each subunit of each network module. The available choices depend on the type of network modules that are configured in the Gateway Configuration window.

**Step 8**  
From the drop-down list boxes, choose the type of VICs that are installed in each subunit and click Save. The window updates to add links for configuring endpoint information and ports for the chosen type of VICs.

**Step 9**  
Click an endpoint identifier (for example, 1/0/0) to configure device protocol information and add ports for the installed types of VICs. See the related topics for links to the detailed instructions.
Step 10  To reset the gateway and apply the changes, click Reset.

Step 11  Continue configuring endpoint information and ports as needed.

Step 12  After you finish configuring the endpoint and adding ports, you need to add the MGCP gateway device to a route group/route list or assign a route pattern to the gateway, so calls can be routed to the gateway.

Note  You need to add the MGCP gateway to a route pattern only for outbound calling.

Related Topics
- Add FXS ports to MGCP gateway, on page 525
- Add FXO ports to MGCP gateway, on page 526
- Add digital access T1 ports to MGCP gateway, on page 527
- Add digital access PRI device to MGCP gateway, on page 528
- Add BRI port to MGCP gateway, on page 528
- Add non-IOS MGCP gateway, on page 530

Add ports to MGCP gateway

The device protocols and port types that can be configured on MGCP gateways vary by the type of installed voice interface cards.

Related Topics
- Add FXS ports to MGCP gateway, on page 525
- Add FXO ports to MGCP gateway, on page 526
- Add digital access T1 ports to MGCP gateway, on page 527
- Add digital access PRI device to MGCP gateway, on page 528
- Add BRI port to MGCP gateway, on page 528

Add FXS ports to MGCP gateway

You can use Foreign Exchange Station (FXS) ports to connect to any POTS device. Use this procedure to configure FXS ports on an MGCP gateway.

Before You Begin

You must add an MGCP gateway before configuring ports.

Procedure

Step 1  To display the Find and List Gateways window, choose Device > Gateway or skip to Step 4, on page 525 if you have already located the MGCP gateway to which you want to add FXS ports.

Step 2  Enter the appropriate search criteria to locate the MGCP gateway to which you want to add FXS ports.

Step 3  Click the name of the desired gateway to display its MGCP configuration settings and endpoint identifiers.

Step 4  From the Gateway Configuration window, click the endpoint identifier for the FXS VIC that you want to configure.
The window refreshes and displays the Gateway Configuration window.

**Step 5** Enter the appropriate Gateway Information and Port Information settings. See the following for details about these fields:

a) Table 80: FXS/FXO port configuration settings, on page 467  
b) Table 84: POTS port configuration settings, on page 515

**Step 6** Click Save.

**Note** After you insert a POTS port, the window refreshes and displays the POTS port information at the bottom of the window. An Add a new DN link displays below the new port.

**Step 7** Click Add a new DN to add directory numbers to the POTS port or, if you configured another type of port, go to **Step 9**, on page 526.

**Step 8** To return to the main MGCP gateway configuration window for the gateway to which you just added the ports, choose Back to MGCP Configuration in the Related Links drop-down list box and click Go.

**Step 9** To reset the gateway and apply the changes, click Reset.

**Step 10** Repeat **Step 4**, on page 525 through **Step 8**, on page 526 to add additional FXS ports.

---

**Related Topics**

- About directory number setup, on page 263  
- Gateway setup, on page 433

**Add FXO ports to MGCP gateway**

You can use Foreign Exchange Office (FXO) ports for connecting to a central office or PBX. Use this procedure to add and configure FXO ports for loop start or ground start on an MGCP gateway.

**Note** Cisco Unified Communications Manager assumes all loop-start trunks lack positive disconnect supervision. Configure trunks with positive disconnect supervision as ground start, so active calls can be maintained during a Cisco Unified Communications Manager server failover.

**Before You Begin**

You must add an MGCP gateway before configuring ports.

**Procedure**

**Step 1** To display the Find and List Gateways window, choose **Device > Gateway** or skip to **Step 4**, on page 526 if you have already located the MGCP gateway to which you want to add FXO ports.

**Step 2** Enter the appropriate search criteria to locate the MGCP gateway to which you want to add FXO ports and click Find. The search results window displays.

**Step 3** Click the name of the desired gateway to display its MGCP configuration settings and endpoint identifiers.

**Step 4** From the MGCP Configuration window, click the endpoint identifiers of the FXO port that you want to configure.

**Step 5** From the Port Type drop-down list box, choose either Ground Start or Loop Start.
You must choose the same port type for both endpoint identifiers of the VIC-2FXO port. If you choose different port types, a message displays.

**Step 6** Enter the appropriate Gateway Configuration and Port Information settings. See the following for details about these fields:

a) Table 80: FXS/FXO port configuration settings, on page 467  
b) Table 85: Loop-start port configuration settings, on page 517  
c) Table 86: Ground-start port configuration settings, on page 518

**Step 7** Click Save.

**Step 8** To return to the main MGCP gateway configuration window for the gateway to which you just added the ports, choose Back to MGCP Configuration in the Related Links drop-down list box and click Go.

**Step 9** To reset the gateway and apply the changes, click Reset.

**Step 10** To add more FXO ports, repeat Step 4, on page 526 though Step 7, on page 527.

### Related Topics

Gateway setup, on page 433

---

**Add digital access T1 ports to MGCP gateway**

Use this procedure to add Digital Access T1 (T1-CAS) ports to an MGCP gateway.

### Procedure

**Step 1** To display the Find and List Gateways window, choose Device > Gateway or skip to Step 4 if you have already located the MGCP gateway to which you want to add T1-CAS ports.

**Step 2** To locate the MGCP gateway to which you want to add a Digital Access T1 (T1-CAS) port, enter the appropriate search criteria.

**Step 3** To display its MGCP configuration settings and endpoint identifiers, click the name of the desired gateway.

**Step 4** From the Gateway Configuration window, click the endpoint identifier of the Digital Access T1 (T1-CAS) port that you want to configure. 
   In the Device Protocol drop-down list box that displays, choose Digital Access T1 and click Next. 
   See the related topics for links to find the appropriate settings for the port type that you choose.

**Step 5** Enter the appropriate Gateway Configuration settings. 
   See the Table 82: Digital access T1 port configuration settings, on page 495 for details.

**Step 6** Click Save.

**Step 7** To reset the gateway and apply the changes, click Reset.

### Related Topics

Gateway setup, on page 433  
Port setup, on page 467
Add digital access PRI device to MGCP gateway

Procedure

Step 1  To display the Find and List Gateways window, choose Device > Gateway or skip to Step 4, on page 525 if you have already located the MGCP gateway to which you want to add a port.

Step 2  To locate the MGCP gateway to which you want to add a T1 PRI or E1 PRI port, enter the appropriate search criteria.

Step 3  To display the configuration information for the selected gateway, click the name of the desired gateway in the list.

Step 4  From the Gateway Configuration window, click the endpoint identifier of the T1 PRI or E1 PRI port that you want to configure.

Step 5  Configure the T1 PRI or E1 PRI device protocol settings. See the Table 81: Digital access PRI port configuration settings, on page 475 for detailed field descriptions.

Step 6  Click Save.

Step 7  To reset the gateway and apply the changes, click Reset.

Related Topics

Gateway setup, on page 433

Add BRI port to MGCP gateway

The device protocols and port types that you can configure on MGCP gateways vary by the type of installed voice interface cards (VICs). This section contains the procedures for adding a BRI port to an MGCP gateway.

Procedure

Step 1  To display the Find/List Gateways window, choose Device > Gateway, or if you have already located the MGCP gateway to which you want to add a port, skip to Step 4, on page 526.

Step 2  To locate the MGCP gateway to which you want to add a BRI port, enter the appropriate search criteria.

Step 3  To display the configuration information for the chosen gateway, click the name of the desired gateway in the list.

Step 4  From the MGCP Configuration window, click the endpoint identifier of the BRI port that you want to configure.

Step 5  Configure the BRI device protocol settings. See the Table 83: BRI port configuration settings, on page 502 for detailed field descriptions.

Step 6  Click Save.

Step 7  To apply the changes, reset the gateway.

Related Topics

Gateway setup, on page 433
Add Cisco IOS SCCP gateway

Use the following procedure to add and configure a Cisco IOS SCCP gateway to Cisco Unified Communications Manager. The following Cisco IOS gateways support SCCP:

- Cisco IOS 269x Gateways
- Cisco IOS 3725 and 3745 Gateways
- Cisco VG224 Gateway

Before You Begin

Configure a Cisco IOS SCCP gateway by adding the gateway first to Cisco Unified Communications Manager. Afterward, configure the gateway by using the Cisco IOS command-line interface (CLI). For procedures and commands that are required to perform this configuration, see the configuration documentation that is supplied with the gateway.

Procedure

Step 1  Choose Device > Gateway.  
The Find and List Gateway window displays.

Step 2  Click Add New.  
The Add a New Gateway window displays.

Step 3  From the Gateway Type drop-down list box, choose one of the following SCCP gateways:
   a) Cisco IOS 269x  
   b) Cisco IOS 3725 and 3745

Step 4  From the Protocol drop-down list box, choose SCCP.  
Cisco IOS SCCP gateways support SCCP for interfacing to the PSTN or other non-IP devices, depending on the gateway model and the type of installed network modules and voice interface cards (VICs). A subsequent web window provides configuration for the interface.

Step 5  Click Next.  
The Gateway Configuration window displays for this SCCP gateway.

Step 6  Enter the appropriate settings and choose the type of network modules that are installed in each slot, as described in Table 79: Cisco IOS SCCP gateway configuration settings, on page 465, including any product-specific configuration settings.

Step 7  Click Save.  
The Gateway Configuration window updates and displays drop-down list boxes with options for configuring the type of voice interface cards (VICs) in each subunit of each network module.

   The available choices depend on the type of network modules that are configured in the Gateway Configuration window.

Step 8  From the drop-down list boxes, choose the type of VICs that are installed in each subunit and click Save.  
The window updates to add links for configuring endpoint information and ports for the chosen type of VICs.
**Add gateway to Cisco Unified Communications Manager**

**Step 9** Click an endpoint identifier (for example, 1/0/0) to configure device protocol information, add ports for the installed types of VICs, and add FXS/BRI port to a SCCP gateway. See the related topics for details of configuring the analog phones.

**Step 10** Reset the gateway to apply the changes.

**Step 11** Continue configuring endpoint information and ports as needed.

---

**Related Topics**

- Cisco Unified IP Phone setup, on page 537
- Set up speed-dial buttons or abbreviated dialing, on page 582

---

**Add non-IOS MGCP gateway**

Use the following procedure to add the following non-IOS Cisco MGCP gateways to Cisco Unified Communications Manager:

- Cisco Catalyst 6000 E1 VoIP Gateway
- Cisco Catalyst 6000 T1 VoIP Gateway

**Procedure**

**Step 1** To display the Find and List Gateways window, choose Device > Gateway.

**Step 2** Click the Add New button.
The Add a New Gateway window displays.

**Step 3** From the Gateway Type drop-down list box, choose one of the following digital gateways and click Next:
- a) Cisco Catalyst 6000 E1 VoIP Gateway
- b) Cisco Catalyst 6000 T1 VoIP Gateway

**Step 4** From the drop-down list box, choose the appropriate device protocol for the type of interfaces that you are configuring on the gateway. The available choices vary according to gateway model:
- a) Cisco Catalyst 6000 T1 VoIP Gateway—Choose either Digital Access PRI or Digital Access T1.
- b) Cisco Catalyst 6000 E1 VoIP Gateway—The Digital Access PRI device protocol automatically gets chosen, and the Gateway Configuration window displays. Skip to Step 6, on page 530.

**Step 5** Click Next.
The Gateway Configuration window displays.

**Step 6** Enter the appropriate settings, depending on whether you are configuring a Digital Access PRI interface or a Digital Access T1 interface as described in following sections:
- a) Table 81: Digital access PRI port configuration settings, on page 475
b) **Table 82: Digital access T1 port configuration settings**, on page 495

**Step 7**

Click Save.

**Step 8**

If you are configuring a Digital Access T1 interface on a Catalyst 6000 T1 VoIP Gateway, in the Ports pane that displays on the left side of the window, click Add a New Port link to configure ports.

**Step 9**

To reset the gateway and apply the changes, click Reset.

---

**Related Topics**

- Gateway setup, on page 433
- Add digital access T1 ports to MGCP gateway, on page 527

---

**Add Cisco IOS H.323 gateway**

Perform the following procedures to add a Cisco IOS H.323 Gateway to Cisco Unified Communications Manager.

---

**Note**

After a gateway is registered with Cisco Unified Communications Manager, gateway registration status may display in Cisco Unified Communications Manager Administration as unknown.

---

**Before You Begin**

Before configuring a Cisco IOS H.323 gateway for use with Cisco Unified Communications Manager, you must configure the gateway by using the Cisco IOS command-line interface (CLI). Compared to MGCP gateways, H.323 gateways require more configuration on the gateway because the gateway must maintain the dial plan and route pattern. For procedures and commands that are required to perform this configuration, see the configuration documentation that is supplied with the gateway.

**Procedure**

---

**Step 1**

To display the Find and List Gateways window, choose **Device > Gateway**.

**Step 2**

Click the Add New button.

The Add a New Gateway window displays.

**Step 3**

From the Gateway Type drop-down list box, choose H.323 Gateway.

**Step 4**

Click Next.

**Step 5**

Enter the appropriate settings as described in **Table 76: H.323 gateway configuration settings**, on page 438.

**Step 6**

Click Save.

**Step 7**

To reset the gateway and apply the changes, click Reset.

---

**Related Topics**

- Gateway setup, on page 433
Add analog access gateway and ports

Perform the procedure in this section to add and configure ports for the Cisco Catalyst 6000 24 Port FXS Gateway.

Procedure

Step 1  To display the Find and List Gateways window, choose Device > Gateway.

Step 2  Click the Add New button.
The Add a New Gateway window displays.

Step 3  From the Gateway type drop-down list box, choose Cisco Catalyst 6000 24 Port FXS Gateway.

Step 4  Click Next.
The Gateway Configuration window displays.

Step 5  Enter the appropriate settings, as described in the Table 77: Analog access gateway configuration settings, on page 459.

Step 6  Click Save.

Step 7  To add a port to this gateway, click the Add a New Port link in the Ports pane that displays on the left side of the window.
The Port Configuration window displays.

Step 8  From the drop-down list box, choose POTS as the port type and click Next.

Step 9  Enter the appropriate port configuration settings as described in the Table 84: POTS port configuration settings, on page 515.

Step 10  Click Save.
If you have inserted POTS ports, the window refreshes and displays the POTS port in the list on the left side of the window. An Add DN link displays to the right of the new port.

Step 11  To add a directory numbers to a POTS port, click Add DN.

Step 12  After you finish adding POTS ports and configuring directory numbers for the POTS ports, you can return to the Gateway Configuration window. In the Related Links drop-down list box, choose Configure Device and click Go.

Step 13  To apply the changes, click Reset.

Related Topics

About directory number setup, on page 263
Gateway setup, on page 433

Add Cisco VG248 analog phone gateway

The Cisco VG248 Analog Phone Gateway, a standalone, rack-mounted, 48-FXS port product, allows on-premise analog telephones, fax machines, modems, voice-messaging systems, and speakerphones to register with one Cisco Unified Communications Manager cluster.
The Cisco VG248 connects to a Cisco Unified Communications Manager by using the Skinny Client Control Protocol to allow for enhanced features.

Cisco Unified Communications Manager recognizes the Cisco VG248 as a gateway device, called a "Cisco VG248 Gateway." Additionally, Cisco Unified Communications Manager treats each of the 48 ports as an individual device, similar to a Cisco Unified IP Phone, called a "Cisco VGC Phone."

Use the following procedure to add a Cisco VG248 Gateway and to add and configure ports to the gateway.

**Procedure**

**Step 1**  
To display the Find and List Gateways window, choose **Device > Gateway**.

**Step 2**  
Click the Add New button.  
The Add a New Gateway window displays.

**Step 3**  
From the Gateway type drop-down list box, choose Cisco VG248 Gateway.

**Step 4**  
Click Next.  
The Gateway Configuration window displays.

**Step 5**  
Enter the appropriate settings, as described in the Table 78: Cisco VG248 Gateway configuration settings, on page 464.

**Step 6**  
From the Configured Slots, VICs and Endpoints drop-down list box, choose 48_PORTS.

**Step 7**  
Click Save.  
The ports 0 through 48 display in the Configured Slots, VICs, and Endpoints area.

**Step 8**  
Click a port.  
The Phone Configuration window displays and lists the phone model as Cisco VGCPhone. From the Gateway Configuration window, the MAC address automatically displays.

**Step 9**  
Enter the appropriate settings. See the related topics link to configuring speed-dial buttons or abbreviated dialing for more information.

**Step 10**  
Click Save.

**Step 11**  
To configure a directory number for the port, click the Add a New DN link that displays in the Association Information area on the left side of the window.  
The Directory Number Configuration window displays. For information about adding and configuring directory numbers, see the related topics.

**Step 12**  
To configure more ports for the gateway, from the Related Link drop-down list box, choose the Back to Gateway link and click Go.  
The Gateway Configuration window displays. To configure the phone settings and directory numbers for additional ports, repeat **Step 8, on page 533** through **Step 11, on page 533**.

When you configure port 1, the Create all new ports like port 1 button displays at the top of the Gateway Configuration window. This button allows you to configure ports 2 through 48 with the same parameters and settings as port 1, but only if ports 2 through 48 are not configured.

**Step 13**  
To apply the changes, click Reset.

**Related Topics**

  * About directory number setup, on page 263
Gateway and port modification

Using Cisco Unified Communications Manager, you can synchronize, as well as update gateways and ports for all gateway types.

Related Topics
- Synchronize gateway, on page 534
- Update gateways and ports, on page 534

Synchronize gateway

To synchronize a gateway with the most recent configuration changes, perform the following procedure, which applies 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 Device > Gateway.
The Find and List Gateways window displays.
Step 2 Choose the search criteria to use.
Step 3 Click Find.
The window displays a list of gateways that match the search criteria.
Step 4 Check the check boxes next to the gateways that you want to synchronize. To choose all gateways in the window, check the check box in the matching records title bar.
Step 5 Click Apply Config to Selected.
The Apply Configuration Information dialog displays.
Step 6 Click OK.

Related Topics
- Gateway setup, on page 433

Update gateways and ports

Complete the following steps to update a gateway or reconfigure gateway ports from Cisco Unified Communications Manager.

Procedure

Step 1 Choose Device > Gateway.
The Find and List Gateways window displays.

**Step 2**  To locate a specific gateway, enter search criteria.

**Step 3**  Click Find.

A list of discovered devices displays.

**Step 4**  Click the Device Name of the gateway that you want to update.

The Gateway Configuration window displays.

**Step 5**  Update the appropriate gateway or port settings as described in the related topics links.

To access gateway ports, click the icon of the gateway port or the MGCP endpoint link on the left side of the configuration window for the chosen gateway.

**Step 6**  Click Save.

**Step 7**  To apply the changes, click Reset to reset the gateway.

---

**Related Topics**

- Gateway setup, on page 433
- MGCP gateway settings, on page 435
- Analog access gateway settings, on page 458
- Port setup, on page 467
- FXS/FXO port settings, on page 467
- Digital access PRI port settings, on page 475
- Digital access T1 port settings, on page 495
Gateway and port modification
Cisco Unified IP Phone setup

This chapter provides information about working with and configuring Cisco Unified IP Phones in Cisco Unified Communications Manager Administration.

- About Cisco Unified IP Phones and device setup, page 538
- Phone setup, page 539
- Phone deletion preparation, page 540
- Phone settings, page 541
- Phone settings migration, page 570
- Speed-dial and abbreviated-dial setup, page 570
- BLF speed dial setup, page 576
- BLF directed Call Park setup, page 576
- Set up Cisco Unified IP Phone, page 577
- Migrate existing phone settings to another phone, page 579
- Synchronize phone, page 581
- Set up speed-dial buttons or abbreviated dialing, page 582
- Set up IP phone services, page 583
- Service URL button setup, page 585
- Copy phone record to remote destination profile, page 586
- Modify custom phone button template button items, page 587
- Find actively logged-in device, page 588
- Find remotely logged-in device, page 589
- Display phone MAC address, page 590
About Cisco Unified IP Phones and device setup

Cisco Unified IP Phones as full-featured telephones can plug directly into your IP network. You use the Cisco Unified Communications Manager Administration Phone Configuration window to configure the following Cisco Unified IP Phones and devices:

- Cisco Unified IP Phone 7900 family for both SCCP and SIP
- Cisco Unified IP Phone 9951 or 9971
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 6900 family.
- Cisco IP Video Phone 7985
- Cisco Unified IP SIP Phone 3911
- Cisco IP Phone 30 VIP and Cisco IP Phone 30 SP+
- Cisco IP Phone 12 S, Cisco IP Phone 12 SP, Cisco IP Phone 12 SP+
- H.323 clients
- Computer Telephony Integration (CTI) ports
  
  Be aware that CTI ports may not be associated with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists. If a DN is a member of a line group or hunt list, that DN cannot get associated with a CTI port that you configure with the Phone Configuration window.

- Cisco IP Communicator, Cisco Unified Personal Communicator, and Cisco Unified Mobile Communicator
- Cisco ATA 186 Analog Telephone Adaptor
- Third-party SIP Device (Basic) and (Advanced)
- IP-STE
- Cisco VG248 and VG224 ports (analog phones)

You configure the Cisco VG248 and VG224 analog phone gateways from the Gateway Configuration window of Cisco Unified Communications Manager Administration. From this window, you configure the gateway analog phone ports (doing this takes you to the Phone Configuration window). When you want to update the VG248 and VG224 ports, use the Phone Configuration window.

See topics related to the Cisco Unified IP Phones in the Cisco Unified Communications Manager System Guide lists the configuration steps for Cisco Unified IP Phones that support SIP.

Related Topics

- Gateway setup, on page 433
- Non-Cisco SIP phones setup, on page 877
- Third-party SIP phone setup process, on page 877
Phone setup

In Cisco Unified Communications Manager Administration, use the Device > Phone menu path to configure phones.

Finding phones tips

The Cisco VG248 and VG224 Analog Phone Gateways will not display when you search for phones. You can search for the Cisco VG248 and VG224 Analog Phone ports from the Find and List Phones window of Cisco Unified Communications Manager Administration.

Tip

For methods to limit your search, see the related topics section and the Cisco Unified Communications Manager System Guide.

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.

Phone configuration tips

When you add a new phone, you can choose a phone template that was created by the Bulk Administration Tool to configure automatically some of the phone configuration settings, based on the template.

For each phone device type, the Phone Configuration window displays either Device is trusted or Device is not trusted, along with a corresponding icon. The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.
The Product-Specific Configuration section contains model-specific fields that the phone manufacturer defines. Cisco Unified Communications Manager dynamically populates the fields with default values. To view field descriptions and help for product-specific configuration items, click the “?” question icon in the Product Specific Configuration area to display help in a popup window.

If you need more information, see the documentation for the specific phone that you are configuring or contact the manufacturer.

Select the "Override Common Settings" box for any corresponding setting in the Product Specific Configuration area that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1) Device Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.

**Phone reset tips**

For instructions on how to reset a phone, see the descriptions of the Reset Selected and Reset buttons. You do not have to reset a Cisco Unified IP Phone after you add a directory number or update its settings for your changes to take effect. Cisco Unified Communications Manager automatically performs the reset; however, you can reset a Cisco Unified IP Phone at any time by using the following procedure.

**Note**

If a call is in progress, the phone does not reset until the call completes.

You can also updating the phone with the latest configuration changes by using the least-intrusive method.

**Related Topics**

- GUI buttons and icons, on page 18
- Gateway setup, on page 433
- Cisco Unified IP Phone setup, on page 537
- Phone settings, on page 541
- Set up Cisco Unified IP Phone, on page 577
- Synchronize phone, on page 581
- Find actively logged-in device, on page 588

**Phone deletion preparation**

Before you delete the phone, determine whether the directory number that is associated with the phone needs to be removed or deleted. To remove the directory number before deleting the phone; otherwise, the directory number remains in the Cisco Unified Communications Manager database when the phone gets deleted.

You can view the directory numbers that are assigned to the phone from the Association Information area of the Phone Configuration window. You can also choose Dependency Records from the Related Links drop-down list box in the Phone 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.
Phone settings

The following table describes the available settings in the Phone Configuration window.

Table 89: Phone settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Information | This field displays the name of the active firmware load if the Cisco Unified IP Phone has registered with Cisco Unified Communications Manager. In some cases, the Active Load ID field displays “Unknown.” For example, Cisco Unified Communications Manager Administration might display “Unknown” in the Active Load ID field for any of the following circumstances:  
  • For SCCP phones, when the phone is a Cisco Unified IP Phone 7940 (SCCP), 7960 (SCCP), or 7985 (SCCP), because these phone models do not support the necessary version of SCCP.  
  • For SCCP and SIP phones, when the phone is any third-party phone.  
  • When Cisco Unified Communications Manager cannot determine the status of the phone. |
| Active Load ID  | 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 CM.  
  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. |
| Device is Active | Select whether the device is trusted or not trusted. You can configure this setting for analog phones using SCCP, and for some third-party endpoints. |
## Field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>

### MAC Address

Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones (hardware phones only). Make sure that the value comprises 12 hexadecimal characters.

For information on how to access the MAC address for your phone, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model.

**Cisco VG248 Analog Phone Gateway:**

The MAC address for the Cisco VG248 gateway specifies the endpoint from the Gateway Configuration window of Cisco Unified Communications Manager Administration.

Only one MAC address exists for the Cisco VG248 Analog Phone Gateway. All 48 ports share the same MAC address. Cisco Unified CM requires unique MAC addresses for all devices.

Cisco Unified Communications Manager converts the MAC address for each device by

- Dropping the first two digits of the MAC address
- Shifting the MAC address two places to the left
- Adding the two-digit port number to the end of the MAC address (to the right of the number)

**EXAMPLE:**

MAC Address for the Cisco VG248 is 000039A44218

the MAC address for registered port 12 in the Cisco Unified Communications Manager is 0039A4421812

**Cisco VG224 Analog Phone Gateway:**

You can configure a Cisco VG224 gateway as an MGCP gateway or an SCCP gateway. When it is configured as an SCCP gateway, it can have 24 analog phone endpoints. When it is configured this way, it functions similarly to an IOS SCCP gateway. The MAC address for each individual phone gets calculated by using a formula that considers the slot position, subunit, port, and the last 10 characters of the original MAC address.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter a name to identify software-based telephones, H.323 clients, and CTI ports. For device names that are not based on a MAC address, as a general rule, you can enter 1 to 15 characters comprised of alphanumeric characters (a-z, A-D, 0-9). In most cases you can use dot (.), dash (-), and underscore (_) as well.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Because the rules for the device name field depend on the device type, Cisco recommends that you see the product documentation to determine which character set is valid for your device, as well as the number of characters allowed. For example, when you configure the device name for the Cisco Unified Personal Communicator, make sure that the name starts with UPC.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Ensure that the device name of a Cisco Unified Mobile Communicator does not exceed 15 characters. If the device name of a Cisco Unified Mobile Communicator exceeds 15 characters, migration of this device will fail upon upgrade to a different release of Cisco Unified Communications Manager. If an existing Cisco Unified Mobile Communicator device name specifies a longer name, shorten the device name to 15 or fewer characters. Cisco Unified Mobile Communicator supports dual mode phones. The preceding limit of 15 characters also applies to Cisco Unified Mobile Communicator dual mode. When the MI for a dual mode phone is longer than 15 characters, the cellular network rejects the phone registration.</td>
</tr>
<tr>
<td>Description</td>
<td>Identify the purpose of the device. You can enter the user name (such as John Smith) or the phone location (such as Lobby) in this field. For Cisco VG248 gateways, begin the description with VGC&lt;mac address&gt;. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose the device pool to which you want this phone assigned. The device pool defines sets of common characteristics for devices, such as region, date/time group, and softkey template.</td>
</tr>
<tr>
<td>Common Device Configuration</td>
<td>Choose the common device configuration to which you want this phone assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Configure the common device in the Common Device Configuration window. To see the common device configuration settings, click the View Details link.</td>
</tr>
<tr>
<td>Phone Button Template</td>
<td>Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button. Cisco Unified CM does not make this field available for H.323 clients or CTI ports.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Softkey Template</td>
<td>Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. Leave this field blank if the common device configuration contains the assigned softkey template.</td>
</tr>
<tr>
<td>Common Phone Profile</td>
<td>From the drop-down list box, choose a common phone profile from the list of available common phone profiles.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>From the drop-down list box, choose the appropriate calling search space (CSS). A calling search space comprises a collection of partitions that are searched to determine how a dialed number should be routed. The calling search space for the device and the calling search space for the directory number get used together. The directory number CSS takes precedence over the device CSS. For more information, see the <em>Cisco Unified Communications Manager System Guide</em>. <strong>Note</strong> When set to <code>&lt;none&gt;</code>, Unified CM uses the device mobility calling search space, which is configured on the device pool.</td>
</tr>
<tr>
<td>AAR Calling Search Space</td>
<td>Choose the appropriate calling search space for the device to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.</td>
</tr>
</tbody>
</table>
| Media Resource Group List     | Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List.  
  If you choose `<None>`, Cisco Unified CM uses the Media Resource Group List that is defined in the device pool.  
  For more information, see the *Cisco Unified Communications Manager System Guide*.                                                                 |
| User Hold MOH Audio Source    | To specify the audio source that plays when a user initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays.                                                                                                                        
  If you do not choose an audio source, Cisco Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**. |
### Field | Description
---|---
**Network Hold MOH Audio Source** | To specify the audio source that is played when the network initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Media Resources > Music On Hold Audio Source.  
**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 Cisco Unified IP Phone. A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this Cisco Unified IP Phone consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP. To configure a new location, use the System > Location menu option. For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.  
**AAR Group** | Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Cisco Unified CM uses the AAR group that is associated with Device Pool or Line.  
**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 to support users, including language and font. Cisco Unified CM makes this field available only for phone models that support localization. **Note** If no user locale is specified, Cisco Unified CM uses the user locale that is associated with the device pool. If the users require that information be displayed (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 Manager Locale Installer documentation.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Network Locale | From the drop-down list box, choose the locale that is associated with the phone. The network locale contains a definition of the tones and cadences that the phone in a specific geographic area uses. Cisco Unified CM makes this field available only for phone models that support localization.  
**Note** If no network locale is specified, Cisco Unified CM uses the network locale that is associated with the device pool.  
If users require that country-specific tones be played (on the phone), verify that the locale is installed before configuring the network locale. See the *Cisco Unified Communications Manager* Locale Installer documentation. |
| Built In Bridge | Enable or disable the built-in conference bridge for the barge feature by using the Built In Bridge drop-down list box (choose On, Off, or Default).  
**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 7940 and 7960 phones when the device security mode is set to encrypted.  
For more configuration information, see the *Cisco Unified Communications Manager Features and Services Guide*. You can also see the *Cisco Unified Communications Manager Security Guide* for more information. |
<p>| Privacy       | For each phone that wants Privacy, choose On in the Privacy drop-down list box. For more configuration information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Mobility Mode        | From the drop-down list box, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device. Click View Current Device Mobility Settings to display the current values of these device mobility parameters:  
  • Cisco Unified Communications Manager Group  
  • Roaming Device Pool  
  • Location  
  • Region  
  • Network Locale  
  • AAR Group  
  • AAR Calling Search Space  
  • Device Calling Search Space  
  • Media Resource Group List  
  • SRST  
  For more configuration information, see the *Cisco Unified Communications Manager Features and Services Guide*. |
| Signaling Port              | This field applies only to H.323 devices. The value designates the H.225 signaling port that this device uses. Default value specifies 1720. Valid values range from 1 to 65535.                                            |
| Video Capabilities          | This check box turns video capabilities on and off.                                                                                                                                                         |
| Owner User ID               | From the drop-down list box, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device. Assigning a user ID to the device also moves the device from "Unassigned Devices" to "Users" in the License Usage Report.  
  **Note** Do not configure this field if you are using extension mobility. Extension mobility does not support device owners. |
| Mobility User ID            | From the drop-down list box, choose the user ID of the person to whom this dual-mode phone is assigned.                                                                                                          |
|                             | **Note** The Mobility User ID configuration gets used for the Mobile Connect and Mobile Voice Access features for dual-mode phones. The Owner User ID and Mobility User ID can differ. |
The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. From the Phone Personalization drop-down list box, choose one of the following options:

- **Disabled**—The user cannot customize the Cisco Unified IP Phone by using Phone Designer.
- **Enabled**—The user can use Phone Designer to customize the phone.
- **Default**—The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window.

You must install and configure Phone Designer, so the phone user can customize the phone. Before you install and configure Phone Designer, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer documentation. For more information on Phone Designer, see the Phone Designer documentation at:


From the drop-down list box, choose how the phone will support the services:

- **Internal**—The phone uses the phone configuration file to support the service. Choose this option or Both for Cisco-provided default services where the Service URL has not been updated; that is, the service URL indicates Application:Cisco/<name of service>; for example, Application:Cisco/CorporateDirectory.
  
  Choose Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file.

- **External URL**—Choosing External URL indicates that the phone ignores the services in the phone configuration file and retrieves the services from a Service URL.
  
  If you configured a custom Service URL for a service, including a Cisco-provided default service, you must choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the phone.

- **Both**—Choosing Both indicates that the phone support both the services that are defined in the configuration file and external applications that are retrieved from service URLs.
### Field | Description
---|---
Primary Phone | Choose the physical phone that will be associated with the application, such as IP communicator or Cisco Unified Personal Communicator. When you choose a primary phone, the application consumes fewer device license units and is considered an "adjunct" license (to the primary phone). See the *Cisco Unified Communications Manager Features and Services Guide*.  This field applies only to H.323 devices.  
Wait for Far End H.245 Terminal Capability Set | This check box specifies that Cisco Unified CM waits to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. By default, the system checks this check box. To specify that Cisco Unified CM should initiate capabilities exchange, uncheck this check box.
Phone Load Name | Enter the custom software for the Cisco Unified IP Phone. The value that you enter overrides the default value for the current model. For more information about Cisco Unified IP Phone software and configuration, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager, which is specific to the phone model and Unified CM release.
Single Button Barge | From the drop-down list box, enable or disable the Single Button Barge/cBarge feature for this device or choose Default to use the service parameter setting.  
- Off—This setting disables the Single Button Barge/cBarge feature; however, the regular Barge or cBarge features will still work.  
- Barge—This setting enables the Single Button Barge feature.  
- CBarge—This setting enables the Single Button cBarge feature.  
- Default—Uses the Single Button Barge/cBarge setting that is in the service parameter.  
For more configuration information, see the *Cisco Unified Communications Manager Features and Services Guide*.  
Join Across Lines | From the drop-down list box, enable or disable the Join Across Lines feature for this device or choose Default to use the service parameter setting.  
- Off—This setting disables the Join Across Lines feature.  
- On—This setting enables the Join Across Lines feature.  
- Default—This setting uses the Join Across Lines setting that is in the service parameter.
### Field

<table>
<thead>
<tr>
<th>Use Trusted Relay Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:</td>
</tr>
<tr>
<td>- Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.</td>
</tr>
<tr>
<td>- Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
<tr>
<td>- On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.</td>
</tr>
</tbody>
</table>

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Cisco Unified CM 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 *Cisco Unified Communications Manager System Guide* for details of call behavior.

If both TRP and RSVPAgent are needed for the endpoint, Cisco Unified CM 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 CM first tries to find a transcoder that is also designated as a TRP.

See the *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points.

### BLF Audible Alert Setting (Phone Idle)

This setting determines the busy lamp field (BLF) audible alert setting when no current call exists on the BLF DN:

- On—An audible alert sounds.
- Off—No audible alert sounds.
- Default—The configuration in the Service Parameters Configuration window determines the alert option.

### BLF Audible Alert Setting (Phone Busy)

This setting determines the BLF audible alert setting when at least one active call exists on the BLF DN, but no call pickup alerts exist:

- On—An audible alert sounds.
- Off—No audible alert sounds.
- Default—The configuration in the Service Parameters Configuration window determines the alert option.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always Use Prime Line</td>
<td>From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received.</td>
</tr>
<tr>
<td></td>
<td>• On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls.</td>
</tr>
<tr>
<td></td>
<td>• Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.</td>
</tr>
<tr>
<td>Always Use Prime Line for Voice Message</td>
<td>From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.</td>
</tr>
<tr>
<td></td>
<td>• Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified CM always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.</td>
</tr>
<tr>
<td></td>
<td>• Default—Cisco Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.</td>
</tr>
<tr>
<td>Geolocation</td>
<td>From the drop-down list box, choose a geolocation.</td>
</tr>
<tr>
<td></td>
<td>You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.</td>
</tr>
<tr>
<td></td>
<td>You can also choose a geolocation that has been configured with the System &gt; Geolocation Configuration menu option.</td>
</tr>
<tr>
<td>Feature Control Policy</td>
<td>From the drop-down list box, you can choose a feature control policy that has already been configured in the Feature Control Policy configuration window (Device &gt; Device Settings &gt; Feature Control Policy).</td>
</tr>
<tr>
<td>Retry Video Call as Audio</td>
<td>This check box applies only to video endpoints that receive a call. If this phone receives a call that does not connect as video, the call tries to connect as an audio call.</td>
</tr>
<tr>
<td></td>
<td>By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting.</td>
</tr>
<tr>
<td></td>
<td>If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via automatic alternate routing (AAR) and/or route/hunt list.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ignore Presentation Indicators (internal calls only)</td>
<td>Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls. 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. See the translation configuration settings Table 45: Translation pattern settings, on page 252 for more information about the calling line ID presentation and the connected line ID presentation parameters. For more information about call display restrictions, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Allow Control of Device from CTI</td>
<td>Check this check box to allow CTI to control and monitor this device. If the associated directory number specifies a shared line, the check box should be enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.</td>
</tr>
<tr>
<td>Logged into Hunt Group</td>
<td>This check box, which gets checked by default for all phones, indicates that the phone is currently logged in to a hunt list (group). When the phone gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.</td>
</tr>
<tr>
<td>Remote Device</td>
<td>If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device check box in the Phone Configuration window. Checking this check box tells Cisco Unified CM to allocate a buffer for the phone device when it registers and to bundle SCCP messages to the phone. <strong>Tip</strong> Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays for phones that are running SCCP. Most users do not require this option. Cisco Unified CM sends the bundled messages to the phone when the station buffer is full, as soon as it receives a media-related message, or when the Bundle Outbound SCCP Messages timer expires. To specify a setting other than the default setting (100 msec) for the Bundle Outbound SCCP Messages timer, configure a new value in the Service Parameters Configuration window for the Cisco CallManager service. Although 100 msec specifies the recommended setting, you may enter 15 msec to 500 msec. The phone must support SCCP version 9 to use this option. The following phones do not support SCCP message optimization: Cisco Unified IP Phone 7935/7936. This feature may require a phone reset after update.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Protected Device | Check this check box to designate a phone as protected, which enables the phone to play a 2-second tone to notify the user when a call is encrypted and both phones are configured as protected devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are protected and the call occurs over encrypted media.

Checking this check box represents only one of several configuration requirements for the secure indication tone to play. For a detailed description of the secure indication tone feature and the configuration requirements, see the *Cisco Unified Communications Manager Security Guide*.

If you check this check box and the system determines that the call is not encrypted, the phone plays nonsecure indication tone to alert the user that the call is not protected.

Hotline Device | Check this check box to make this device a Hotline device. Hotline devices can only connect to other Hotline devices. 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.

### Caller ID For Calls From This Phone

| Field | Description |
--- | --- |
Calling Party Transformation CSS for Calls from this Phone | From the drop-down list box, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the calling number when this phone initiates a call.

Cisco Unified CM transforms the calling party using the digit transformations configured on the matching calling party transformation pattern when this phone initiates a call. This setting allows you to transform the calling party number before Cisco Unified CM routes the call. For example, a transformation pattern can change a phone extension to an E.164 number. This setting is generally configured when a user dials using a URI instead of digits. Cisco Unified CM allows calling party transformations on various patterns when dialing using digits, this setting provides similar transformation provision even when dialing using a URI.

Use Device Pool Calling Party Transformation CSS (Caller ID for Calls from this Phone) | Check this check box to use the Calling Party Transformation CSS configured at the device pool to which this phone belongs to transform the calling party for calls initiated from this phone. At the device pool, Calling Party Transformation CSS present under Phone Settings is used to transform the calling party for calls initiated from this phone.

Leave this check box unchecked to apply the Calling Party Transformation CSS setting that appears in this configuration window.

Remote Number Transformation |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Party Transformation CSS for Remote Number</td>
<td>From the drop-down list box, choose the calling search space (CSS) that contains the calling party transformation pattern that you want to apply on the remote calling number for calls received on this phone. Cisco Unified CM transforms the remote calling number using the digit transformations configured on the matching calling party transformation pattern before presenting it to this device. For example, a transformation pattern can change remote number in E.164 format to a localized version. This setting can be used to transform the remote connected number for direct calls initiated from this phone. This setting can also be used to transform remote connected number post feature invocation irrespective of the direction of the call. The transformation of a remote connected number is controlled using the service parameter &quot;Apply Transformations On Remote Number” (present under advanced section of Cisco Call Manager service). Refer to this parameter description for more details.</td>
</tr>
<tr>
<td>Use Device Pool Calling Party Transformation CSS for Remote Number (Device Mobility Related Information)</td>
<td>Check this check box to apply the Calling Party Transformation CSS configured at the device pool to which this phone belongs to transform the remote calling and remote connected number. At the device pool, Calling Party Transformation CSS present under Device Mobility Related Information section is used to transform remote calling and remote connected number. Leave this check box unchecked to apply the Calling Party Transformation CSS setting that appears in this configuration window for transforming the remote number.</td>
</tr>
</tbody>
</table>
| Protocol Specific Information | This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box:  
  - None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting.  
  - Batch Processing Mode—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.  
  For more information on packet capturing, see the Troubleshooting Guide for Cisco Unified Communications Manager. |

packet capture mode: Choose one of the following options from the drop-down list box:  
- None—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting.  
- Batch Processing Mode—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.  

For more information on packet capturing, see the Troubleshooting Guide for Cisco Unified Communications Manager.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Capture Duration</td>
<td>This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays. For more information on packet capturing, see the <em>Cisco Unified Communications Manager Troubleshooting Guide</em>.</td>
</tr>
<tr>
<td>SRTP Allowed</td>
<td>As this check box explains, if this flag is checked, IPSec needs to be configured in the network to provide end-to-end security. Failure to do so will expose keys and other information. For more information on SRTP encryption, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Presence Group</td>
<td>Configure this field with the Presence feature. From the drop-down list box, choose a Presence group for the end user. The selected group specifies the devices, end users, and application users that can monitor this 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 <em>Cisco Unified Communications Manager Features and Services Guide</em> for information about configuring permissions between groups and how presence works with extension mobility.</td>
</tr>
<tr>
<td>Device Security Profile</td>
<td>Choose the security profile to apply to the device. You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration. <em>Installing Cisco Unified Communications Manager</em> provides a set of predefined, nonsecure security profiles for auto-registration. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a nonsecure profile. To identify the settings that the profile contains, choose <strong>System &gt; Security Profile &gt; Phone Security Profile</strong>. <strong>Note</strong> The CAPF settings that are configured in the profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacturer-installed certificates (MICs) or locally significant certificates (LSC). See the Cisco Unified Communications Manager Security Guide for more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings.</td>
</tr>
</tbody>
</table>
If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7905, 7912, 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed.

Leave the SIP Dial Rules field set to <None> if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Dial Rules</td>
<td>If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7905, 7912, 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to &lt;None&gt; if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.</td>
</tr>
<tr>
<td>MTP Preferred Originating Codec</td>
<td>From the drop-down list box, choose the codec to use if a media termination point is required for SIP calls.</td>
</tr>
<tr>
<td>Rerouting Calling Search Space</td>
<td>From the drop-down list box, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.</td>
</tr>
<tr>
<td>Out-of-Dialog Refer Calling Search Space</td>
<td>From the drop-down list box, choose an out-of-dialog refer calling search space. Cisco Unified CM uses the out-of-dialog (OOD) Refer Authorization calling search space (CSS) to authorize the SIP out-of-dialog Refer. The administrator can restrict the use of out-of-dialog Refer by configuring the OOD CSS of the Referrer. Refer Primitive rejects the OOD Refer request with a “403 Forbidden” message.</td>
</tr>
<tr>
<td>SUBSCRIBE Calling Search Space</td>
<td>Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified CM routes presence requests that come from the phone. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the phone. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the phone. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Outbound Call Rollover</td>
<td>Use this setting for the Cisco Unified IP Phone 7931.</td>
</tr>
<tr>
<td></td>
<td>• No Rollover—Conference and transfer will not work in this mode. If a user attempts to use either of these features, the phone status displays as &quot;Error Pass Limit.&quot; Choose this setting only if you need to support CTI applications.</td>
</tr>
<tr>
<td></td>
<td>• Rollover Within Same DN—Conferences and call transfers complete by using the same directory number (on different lines). For example, consider a phone that has directory number 1506 that is assigned to both Line 6 and 7. The user has an active call on Line 6 and decides to transfer the call. When the user presses the Transfer button, the call on Line 6 gets placed on hold, and a new call initiates on Line 7 to complete the transfer.</td>
</tr>
<tr>
<td></td>
<td>• Rollover to any line—Conferences and call transfers complete by using a different directory number and line than the original call. For example, consider a phone that has directory number 1507 assigned to Line 8 and directory number 1508 assigned to Line 9. The user has an active call on Line 8 and decides to transfer the call. When the user presses the Transfer button, the call on Line 8 gets placed on hold, and a new call initiates on Line 9 to complete the transfer.</td>
</tr>
<tr>
<td>SIP Profile</td>
<td>Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.</td>
</tr>
<tr>
<td>Digest User</td>
<td>Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security).</td>
</tr>
<tr>
<td></td>
<td>Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window.</td>
</tr>
<tr>
<td></td>
<td>After you save the phone configuration and apply the configuration update to the phone, the digest credentials for the user get added to the phone configuration file.</td>
</tr>
<tr>
<td></td>
<td>For more information on digest authentication, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Media Termination Point Required</td>
<td>Use this field to indicate whether a media termination point is used to implement features that H.323 does not support (such as hold and transfer).</td>
</tr>
<tr>
<td></td>
<td>Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features.</td>
</tr>
<tr>
<td></td>
<td>Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source.</td>
</tr>
<tr>
<td></td>
<td>If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.</td>
</tr>
<tr>
<td>Unattended Port</td>
<td>Check this check box to indicate an unattended port on this device.</td>
</tr>
</tbody>
</table>
### Phone settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require DTMF Reception</td>
<td>For phones that are running SIP and SCCP, check this check box to require DTMF reception for this phone. <strong>Note</strong>: In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.</td>
</tr>
<tr>
<td>RFC2833 Disabled</td>
<td>For phones that are running SCCP, check this check box to disable RFC2833 support.</td>
</tr>
</tbody>
</table>

**Certification Authority Proxy Function (CAPF) Information**

<table>
<thead>
<tr>
<th>Certificate Operation</th>
<th>From the drop-down list box, choose one of the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No Pending Operation — Displays when no certificate operation is occurring (default setting).</td>
<td></td>
</tr>
<tr>
<td>• Install/Upgrade — Installs a new or upgrades an existing locally significant certificate in the phone.</td>
<td></td>
</tr>
<tr>
<td>• Delete — Deletes the locally significant certificate that exists in the phone.</td>
<td></td>
</tr>
<tr>
<td>• Troubleshoot — Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type. By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone.</td>
<td></td>
</tr>
</tbody>
</table>

For more information on CAPF operations, see the *Cisco Unified Communications Manager Security Guide*. 
This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation.

From the drop-down list box, choose one of the following options:

- **By Authentication String**—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone.

- **By Null String**—Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.

- **By Existing Certificate (Precedence to LSC)**—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails.

  At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode.

- **By Existing Certificate (Precedence to MIC)**—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails.

**Note**  The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Mode</td>
<td>This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>By Authentication String</strong>—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone.</td>
</tr>
<tr>
<td></td>
<td>• <strong>By Null String</strong>—Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.</td>
</tr>
<tr>
<td></td>
<td>• <strong>By Existing Certificate (Precedence to LSC)</strong>—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails.</td>
</tr>
<tr>
<td></td>
<td>At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>By Existing Certificate (Precedence to MIC)</strong>—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails.</td>
</tr>
<tr>
<td>Authentication String</td>
<td>If you chose the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Key Size (Bits)** | For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048.

If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete.

**Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.

**Operation Completes by** | This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation.

The values that display apply for the publisher database server.

**Certificate Operation Status** | This field displays the progress of the certificate operation; for example, <operation type>= pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field.

**External Data Locations Information (Leave blank to use default)**

**Information** | Enter the location (URL) of the help text for the information (i) button. Leave this field blank to accept the default setting.

**Directory** | Enter the server from which the phone obtains directory information. Leave this field blank to accept the default setting.

**Note** If you set a Secured Directory URL enterprise parameter in the Enterprise Parameters Configuration window, that value overwrites the value of this field.

**Messages** | Leave this field blank (not used by Cisco Unified Communications Manager).

**Services** | Enter the location (URL) for IP phone services.

**Authentication Server** | Enter the URL that the phone uses to validate requests that are made to the phone web server. If you do not provide an authentication URL, the advanced features on the Cisco Unified IP Phone that require authentication will not function.

By default, this URL accesses a Cisco Unified CM User Options window that was configured during installation.

Leave this field blank to accept the default setting.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Proxy Server             | Enter the host and port (for example, proxy.cisco.com:80) that are used to proxy HTTP requests for access to non-local host addresses from the phone HTTP client. The rule contains two parts for when to use the proxy server parameter:  
|                          | 1 The hostname contains a "."  
|                          | 2 The hostname specifies an IP address in any form.                                                                                                                                                    |
|                          | If you do not configure this URL, the phone attempts to connect directly to the URL. To accept the default setting, leave this field blank.                                                                     |
| Idle                     | Enter the URL that displays on the Cisco Unified IP Phone display when the phone has not been used for the time that is specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes. To accept the default setting, leave this field blank. |
| Idle Timer (seconds)     | Enter the time (in seconds) that you want to elapse before the URL that is specified in the Idle field displays. To accept the value of the Idle URL Timer enterprise parameter, leave this field blank. |
| Secure Authentication URL| Enter the secure URL that the phone uses to validate requests that are made to the phone web server.                                                                                                        |
|                          | **Note** If you do not provide a Secure Authentication URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. By default, this URL accesses a Cisco Unified CM User Options window that was configured during installation. Leave this field blank to accept the default setting. Maximum length: 255 |
| Secure Directory URL     | Enter the secure URL for the server from which the phone obtains directory information. This parameter specifies the URL that secured Cisco Unified IP Phones use when you press the Directory button.  
|                          | **Note** If you do not provide a Secure Directory URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. Leave this field blank to accept the default setting. Maximum length: 255 |
### Field | Description
--- | ---
Secure Idle URL | Enter the secure URL for the information that displays on the Cisco Unified IP Phone display when the phone is idle, as specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes.  
**Note** If you do not provide a Secure Idle URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.  
To accept the default setting, leave this field blank.  
Maximum length: 255

Secure Information URL | Enter the secure URL for the server location where the Cisco Unified IP Phone can find help text information. This information displays when the user presses the information (i) button or the question mark (?) button.  
**Note** If you do not provide a Secure Information URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.  
To accept the default setting, leave this field blank.  
Maximum length: 255

Secure Messages URL | Enter the secure URL for the messages server. The Cisco Unified IP Phone contacts this URL when the user presses the Messages button.  
**Note** If you do not provide a Secure Messages URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.  
To accept the default setting, leave this field blank.  
Maximum length: 255

Secure Services URL | Enter the secure URL for Cisco Unified IP Phone services. The is the location that the secure Cisco Unified IP Phone contacts when the user presses the Services button.  
**Note** If you do not provide a Secure Services URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.  
To accept the default setting, leave this field blank.  
Maximum length: 255

Extension Information

Enable Extension Mobility | Check this check box if this phone supports extension mobility.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Out Profile</td>
<td>This drop-down list box specifies the device profile that the device uses when no one is logged in to the device by using Cisco Extension Mobility. You can choose either Use Current Device Settings or one of the specific configured profiles that are listed. If you select a specific configured profile, the system retains a mapping between the device and the login profile after the user logs out. If you select Use Current Device Settings, no mapping gets retained.</td>
</tr>
<tr>
<td>Log In Time</td>
<td>This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the user logged in displays in this field.</td>
</tr>
<tr>
<td>Log Out Time</td>
<td>This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the system will log out the user displays in this field.</td>
</tr>
<tr>
<td>Configuration File Encryption Symmetric Key Information</td>
<td></td>
</tr>
<tr>
<td>Symmetric Key</td>
<td>Enter a string of hexadecimal characters that you want to use for the symmetric key. Valid characters include numerals, 0-9, and upper/lower case characters, A-F (or a-f). Make sure that you enter the correct bits for the key size; otherwise, Cisco Unified CM rejects the value. Cisco Unified CM supports the following key sizes: • Cisco Unified IP Phones 7905 and 7912 (SIP only)—256 bits • Cisco Unified IP Phones 7940 and 7960 (SIP only)—128 bits Use this string for one-time use only. Every time that you update the configuration settings, you must generate a new key before you apply the configuration changes to the phone. For more information on symmetric key operations for encrypted configuration file downloads, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Generate String</td>
<td>If you want Cisco Unified Communications Manager Administration to generate a hexadecimal string for you, click the Generate String button.</td>
</tr>
<tr>
<td>Revert to Database Value</td>
<td>If you want to restore the value that exists in the database, click this button. This button proves useful if you enter an error in the Symmetric Key field before you save the configuration.</td>
</tr>
<tr>
<td>H.323 Information</td>
<td></td>
</tr>
<tr>
<td>Outgoing Caller ID Pattern</td>
<td>For outgoing calls to the H.323 Client, enter the pattern, from 0 to 24 digits, that you want to use for caller ID.</td>
</tr>
</tbody>
</table>
### Calling Party Selection

Choose the directory number that is sent on an outbound call to the H.323 Client. The following options specify which directory number is sent:

- **Originator**—Send the directory number of the calling device.
- **First Redirect Number**—Send the directory number of the redirecting device.
- **Last Redirect Number**—Send the directory number of the last device to redirect the call.
- **First Redirect Number (External)**—Send the external directory number of the redirecting device.
- **Last Redirect Number (External)**—Send the external directory number of the last device to redirect the call.

### Calling Party Presentation

Choose whether the Cisco Unified CM transmits or blocks caller ID. If you want Cisco Unified CM to send caller ID, choose Allowed. If you do not want Cisco Unified CM to send caller ID, choose Restricted. Default specifies that caller ID does not get sent.

### Display IE Delivery

This check box enables delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service. The default setting checks this check box.

### Redirecting Number IE Delivery Outbound

Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified CM includes the Redirecting Number IE.)

Uncheck the check box to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message.

You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.

**Note** The default setting leaves this check box unchecked.

### Redirecting Number IE Delivery Inbound

Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CM. (The UUIE part of the SETUP message includes the Redirecting Number IE.)

Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco Unified CM.

You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.

**Note** Default leaves the check box unchecked.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gatekeeper Information</strong></td>
<td></td>
</tr>
<tr>
<td>Gatekeeper Name</td>
<td>This field specifies the name of the gatekeeper that controls the H.323 client. Ensure the gatekeeper is configured in Cisco Unified CM before an H.323 client is allowed to specify the gatekeeper in its configuration. Default specifies empty.</td>
</tr>
<tr>
<td>E.164</td>
<td>Always use a unique E.164 number. Do not use null value.</td>
</tr>
<tr>
<td>Technology Prefix</td>
<td>This field specifies a number ending with the # sign that describes the capability of an endpoint in a zone. This field has no impact if via Zone configuration can be used. Default specifies 1#*. Do not use null value.</td>
</tr>
<tr>
<td>Zone</td>
<td>This field specifies the zone name of the zone that the gatekeeper manages. Do not use the following values: same zone name for the H.323 client and trunk; null.</td>
</tr>
<tr>
<td><strong>Associated Mobility Identity</strong></td>
<td></td>
</tr>
<tr>
<td>(mobility identity)</td>
<td>If a mobility identity has already been configured for this device, this area displays the Name and Destination Number of the mobility identity. You can click either value to display the Mobility Identity Information in the Remote Destination Configuration window. &lt;br&gt;<strong>Note</strong> This field displays only after a Cisco Unified Mobile Communicator device has been added. The Cisco Unified Mobile Communicator must be enabled for a mobile phone.</td>
</tr>
<tr>
<td>Add New Mobility Identity</td>
<td>If no mobility identity has been defined for this device, click this link to add a mobility identity. The Remote Destination Configuration window displays, which allows you to add a new mobility identity to associate with this device. &lt;br&gt;<strong>Note</strong> This field displays only after a Cisco Unified Mobile Communicator device has been added.</td>
</tr>
<tr>
<td><strong>Associated Remote Destinations</strong></td>
<td></td>
</tr>
<tr>
<td>(remote destination)</td>
<td>If a remote destination has already been configured for this device, this area displays the Name and Destination Number of the remote destination(s). You can click the values to display the Remote Destination Information in the Remote Destination Configuration window. &lt;br&gt;<strong>Note</strong> This field appears only after a Cisco Unified Mobile Communicator device has been added.</td>
</tr>
<tr>
<td>Add a New Remote Destination</td>
<td>Click this link to add a remote destination to associate with this device. The Remote Destination Configuration window displays, which allows you to add a new remote destination to associate with this device. &lt;br&gt;<strong>Note</strong> This field appears only after a Cisco Unified Mobile Communicator device has been added.</td>
</tr>
<tr>
<td><strong>MLPP Information</strong></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MLPP Domain</td>
<td>Choose an MLPP domain from the drop-down list box for the MLPP domain that is associated with this device. If you leave the None value, this device inherits its MLPP domain from the value that was set in the common device configuration. If the common device configuration does not have an MLPP domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
</tbody>
</table>
| MLPP Indication  | If available, this setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options:  
• Default—This device inherits its MLPP indication setting from the common device configuration.  
• Off—This device does not handle nor process indication of an MLPP precedence call.  
• On—This device does handle and process indication of an MLPP precedence call.  
**Note**  
Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.  
Turning on MLPP Indication (at the enterprise parameter or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device. |
| MLPP Preemption  | Be aware that this setting is not available on all devices. If available, this setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list box, choose a setting to assign to this device from the following options:  
• Default—This device inherits its MLPP preemption setting from the common device configuration.  
• Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.  
• Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.  
**Note**  
Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. |
| Do Not Disturb (DND) |                                                                                                                                              |
| Do Not Disturb   | Check this check box to enable Do Not Disturb on the phone.                                                                                   |
When you enable DND on the phone, this parameter allows you to specify how the DND features handle incoming calls:

- **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 the user can accept the call.

- **Use Common Phone Profile Setting**—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device.

**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.

### 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 gets 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.

### Secure Shell Information
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Shell User</td>
<td>Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include”, %, &amp;, ,, &gt;, and . This field displays when the phone device that you are configuring supports SSH access. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance. See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH credentials to the phone in the clear.</td>
</tr>
<tr>
<td>Secure Shell Password</td>
<td>Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 200 characters. Invalid characters include”, %, &amp;, ,, &gt;, and . Contact TAC for further assistance. See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified CM does not send SSH passwords to the phone in the clear.</td>
</tr>
<tr>
<td>Association Information</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add a new BLF SD</td>
<td>After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to configure busy lamp field/speed dial settings for this phone. When you click the link, the Busy Lamp Field Directed Call Park Configuration window displays for this phone.</td>
</tr>
<tr>
<td>Add a new BLF Directed Call Park</td>
<td>After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this link to configure busy lamp field/directed call park settings for this phone. When you click the link, the Busy Lamp Field Directed Call Park Configuration window displays for this phone. For more information on configuring BLF/Directed Call Park buttons, see the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
</tbody>
</table>

**Product-Specific Configuration Layout**

Model-specific configuration fields that the device manufacturer defines

To view field descriptions and help for product-specific configuration items, click the “?” information icon in the Product Specific Configuration area to display help in a popup dialog box.

If you need more information, see the documentation for the specific device that you are configuring or contact the manufacturer.

Select the “Override Common Settings” box for any corresponding setting in the Product Specific Configuration area that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1) Device Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.

**Related Topics**

- Location setup, on page 107
- Calling search space setup, on page 247
- About translation pattern setup, on page 251
- About directory number setup, on page 263
- Display calling search space, on page 291
- Gateway setup, on page 433
- BLF speed dial setup, on page 576
- Synchronize phone, on page 581
- Set up speed-dial buttons or abbreviated dialing, on page 582
- Service URL button setup, on page 585
- Modify custom phone button template button items, on page 587
Phone settings migration

You can migrate existing phone settings to a different phone.

Related Topics

- Migrate existing phone settings to another phone, on page 579
- Phone migration settings, on page 580

Speed-dial and abbreviated-dial setup

The following table describes the speed-dial button configuration settings. The Speed Dial and Abbreviated Dial Configuration window contains the following sections: speed-dial settings on the phone and abbreviated-dial settings that are not associated with a button. The descriptions in the table apply to both sections.

The system provides a total of 199 speed-dial and abbreviated-dial settings.

**Speed dial settings**

Configure these settings for the physical buttons on the phone.

**Abbreviated dial settings**

Configure these settings for the speed-dial numbers that you access with abbreviated dialing. When the user configures up to 199 speed-dial entries, part of the speed-dial entries can get assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries get used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays on the phone, and the user can access any speed-dial entry by entering the appropriate index (code) for abbreviated dialing.

**Pause in speed dial feature specific settings**

In Cisco Unified Communication Manager, the user can configure Forced Authorization Code (FAC), Client Matter Code (CMC), and post-connect Dual Tone Multifrequency (DTMF) digits as a part of a speed dial number. The Unified CM recognizes the destination address digits, FAC, CMC, and post-connect DTMF digits that are configured as a part of a speed dial number.

The Unified CM uses the following:

1. Destination address digits to route the call
2. FAC digits to authorize the user before routing the call to a particular gateway or a trunk
3. CMC digits for billing before routing the call to a particular gateway or a trunk

The Unified CM sends out post-connect DTMF digits with appropriate pause duration after the call is connected and a media connection is established.

**Note**

Even if the media connection is established before a call is connected, the DTMF digits are sent only after the call is connected.
There are two methods to configure this feature:

- **Method I**: Using comma as a pause and also as a delimiter
- **Method II**: Entering destination address digits, FAC, CMC, and DTMF digits as a continuous string without using any delimiter

### Method I: Using comma as a pause and also as a delimiter

1. **Using comma as a pause**
   
   The users can configure the special character comma (,) within speed dial, which acts as a pause duration of 2 seconds for sending post-connect DTMF digits. The Unified CM pauses for the appropriate duration corresponding to the number of commas entered before sending out DTMF digits to the remote side of the call.

   **Example 1: Reading a Voicemail message**
   
   Without the Pause in Speed dial feature, the user must perform the following to read a voicemail message:
   
   1. Click message button on the phone or 8000 [Voicemail pilot number] to reach the Cisco Unity Server.
   2. Enter 91941420# [PIN] after announcement of 2 seconds after the call is connected.
   3. Enter option 3 to read the latest message after a pause of around 6 seconds (while the operator reads the options) after the PIN is verified.

   With Pause in Speed dial feature, the user can configure speed dial as 8000,91941420#,,,3 and press the speed dial key and read the latest message received. Here, the Unified CM waits for 2 seconds after the call is connected, then sends out the PIN [91941420#] to the Cisco Unity Server and again waits for 6 seconds before sending out the option [3] to the Cisco Unity Server.

2. **Using comma as a delimiter**
   
   A comma can be used as a delimiter in the following cases:
   
   - To separate the FAC from the destination address digits
   - To separate destination address digits and CMC (if FAC is not enabled)
   - To separate the FAC and CMC

   This enables Unified CM to recognize the destination address digits, FAC, CMC, and DTMF digits when user has configured the following:

   1. Overlapping dial patterns [Example: 9.XXXX and 9.XXXXX are overlapping Route patterns]
   2. Variable length dial patterns [Example: 8.1]
   3. Overlapping FAC and CMC [Example of overlapping FAC: 8787, 87879]

### Example 2: Connecting to IVR application over a gateway

If the user wants to reach out to an IVR application over a gateway, to the user must enter FAC and CMC digits to reach the gateway and then send out IVR responses after the call is connected. The manual dialing works as follows:

1. Enter called number: 91886543
2. Enter Forced Authorization Code: 8787
3. Enter Client Matter Code: 5656
4. IVR response 4 seconds after the call is connected: 987989#
Using the Pause in Speed Dial feature, a user can configure speed dial as follows to achieve the same result: 91886543,8787,5656,,987989#

In this example, the Unified CM uses 8787 as FAC, 5656 as CMC before the call is routed to a gateway and sends out IVR response [987989#] 4 seconds after the call is connected.

---

**Note**
Ensure the FAC always precedes the CMC when you configure a speed dial that includes FAC and CMC.

---

**Note**
Ensure to use only a single comma as a delimiter. If more than one comma is configured, the digits after multiple commas are considered as DTMF digits and users are prompted to enter the FAC or CMC manually.

---

**Handling incorrect FAC or CMC when comma is used as a delimiter**

Whenever comma is used as a delimiter and FAC or CMC is configured as a part of speed dial is incorrect or unauthorized to make a particular call then the Unified CM disconnects the call with the following error message on the phone where speed dial is invoked:

*Error: Invalid Code in SpeedDial*

**Method II: Entering main address, FAC, CMC, and DTMF digits as a continuous string without using any delimiter**

With this method, speed dial is configured as a continuous string of digits and Unified CM identifies following components from the digit string:

1. Destination address digits
2. FAC
3. CMC
4. DTMF digits [DTMF digits are sent immediately after the call is connected]

This method allows the user to configure the Pause in Speed Dial feature on Cisco Unified Personal Communicator endpoints which do not have the speed dial option.

**Example 3: Connecting to IVR application, which prompts users to enter responses immediately after call is connected**

If the user wants to reach an IVR application and is required to enter FAC and CMC digits to reach to a gateway and then send out IVR response after call is connected, the manual dialing works as follows:

1. Enter called number: 91886543 [ Using Route Pattern 9.XXXXXXX ]
2. Enter Forced Authorization Code: 8787
3. Enter Client Matter Code: 5656
4. IVR response immediately after the call is connected: 987989#

Using the Pause in Speed Dial feature, a user can configure speed dial as follows to achieve the same result: 9188654387875656987989#

**Handling incorrect FAC or CMC when comma is not used as a delimiter**

Whenever a comma is not used as a delimiter and FAC or CMC is configured as a part of speed dial is incorrect or unauthorized to make a particular call then the Unified CM switches to manual dialing mode from the point of failure.
Example: If FAC entered is incorrect (even if CMC entered is correct), Unified CM switches to manual dialing mode and displays the following error message at the phone:

*Auth code failed: Enter manually*

After receiving this error message, the user must dial out FAC, CMC, and DTMF digits manually.

If FAC entered is correct and validated but CMC entered is incorrect, Unified CM switches to manual dialing mode and displays the following error message at the phone:

*CM code failed: Enter manually*

After receiving this error message, the user must dial CMC and DTMF digits manually.

The following table describes the comparison between using a comma and not using a comma as a delimiter.

### Table 90: Comparison between two methods

<table>
<thead>
<tr>
<th>Method I: Using comma as a delimiter and also as a pause</th>
<th>Method II: Not using comma as a delimiter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can be configured when the customer has</td>
<td>Only preferred for calls made using fixed length route patterns. This method may not work when overlapping route patterns and overlapping FAC and CMC are configured.</td>
</tr>
<tr>
<td>• Overlapping route patterns</td>
<td></td>
</tr>
<tr>
<td>• Variable length dial patterns</td>
<td></td>
</tr>
<tr>
<td>• Overlapping FAC and CMC</td>
<td></td>
</tr>
<tr>
<td>DTMF digits can be sent after appropriate pause</td>
<td>DTMF digits are always sent immediately after the call is connected.</td>
</tr>
<tr>
<td>duration.</td>
<td></td>
</tr>
<tr>
<td>Call is disconnected when invalid FAC or CMC is entered.</td>
<td>For FAC, CMC failure cases, Unified CM switches to manual dialing mode and user gets one more chance to enter correct code.</td>
</tr>
<tr>
<td>Can be used even when FAC and CMC are not required to</td>
<td>Can be used only for the calls made over route patterns where at least one out of FAC and CMC is enabled. This method cannot be used for sending only DTMF digits.</td>
</tr>
<tr>
<td>make calls; that is, can be used for sending only</td>
<td></td>
</tr>
<tr>
<td>DTMF digits.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

Unified CM ensures FAC, CMC, and DTMF digits are not displayed in the phone placed calls history for the calls made using speed dial with the codes configured.

After a call is successful, when the user presses the Redial softkey or dials out from the placed calls history, to the user must dial out FAC, CMC, and DTMF digits manually.

When the Unified CM sends a group of DTMF digits (configured as a part of speed dial) after a pause or after the call is connected, there is a possibility that the Unified CM may out-pulse these DTMF digits quickly for remote application or remote gateway to process.

To prevent this, Unified CM pauses for the duration specified in service parameter "Pause In Speed Dial InterDigit Interval." In the previous example DTMF digits are: 987989#
Unified CM sends out the first DTMF digit, that is, 9, and waits for the duration specified in this service parameter before sending out the next digit, that is, 8. Similarly, it follows the same pattern before sending out each digit.

The following table describes the Speed-dial and abbreviated-dial configuration settings.

### Table 91: Speed-dial and abbreviated-dial configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(number from 1 to 199 in the left column)</td>
<td>This column identifies the speed-dial button on the phone or on the Cisco Unified IP Phone Expansion Module (for example, 1, 2, 3, or 4) or the abbreviated-dial index for abbreviated dial.</td>
</tr>
<tr>
<td>Number</td>
<td>Enter the number that you want the system to dial when the user presses the speed-dial button. You can enter digits 0 through 9, *, #, and +, which is the international escape character. For a Pause in Speed Dial, you can enter comma (,) which can act as a delimiter as well as other pause before sending DTMF digits.</td>
</tr>
<tr>
<td>Label</td>
<td>Enter the text that you want to display for the speed-dial button or abbreviated-dial number. If you are configuring a Pause in Speed Dial, you must add a label so that FAC, CMC, and DTMF digits are not displayed on the phone screen. Cisco Unified Communications Manager does not make this field available for the Cisco Unified IP Phone 7910.</td>
</tr>
<tr>
<td>ASCII Label</td>
<td>This field provides the same information as the Label field, but you must limit input to ASCII characters. Devices that do not support unicode (internationalized) characters display the content of the ASCII Label field.</td>
</tr>
</tbody>
</table>

The following table describes the SIP Phone models and support information.

**Phone Model Support**
### Table 92: SIP Phone Models and Support Information

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Support</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phones 8961, 9951, 9971 using SIP</td>
<td>Fully Supported</td>
<td>• Placed calls history of a phone does not show FAC, CMC, and post-connect DTMF digits for the calls that are placed using the speed dial.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DTMF digits are sent by both out of band and RFC2833 method. In both the cases, users can hear the tone that indicates the DTMF digit is sent.</td>
</tr>
<tr>
<td>Cisco Unified Personal Communicator Clients</td>
<td>Supported using only method II [See Method II section]</td>
<td>• DTMF digits can be sent by both out of band and RFC2833 method.</td>
</tr>
</tbody>
</table>

The following table describes the SCCP Phone models and support information.

### Table 93: SCCP Phone Models and Support Information

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Support</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phones 7906, 7911, 7931, 7941, 7961, 7942, 7962, 7945, 7965, 7970, 7971, 7975 using SCCP</td>
<td>Fully Supported</td>
<td>• Placed calls history of a phone does not show FAC, CMC, and post-connect DTMF digits for the calls placed using the speed dial.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DTMF digits can be sent by both out of band and RFC2833 method. In both the cases, users can hear the tone that indicates the DTMF digit is sent.</td>
</tr>
</tbody>
</table>
### CME and SRST Limitations

When a phone is in the CME (configured as SRST) or SRST mode, for the speed dial calls where a comma is used as a pause duration or as a delimiter, the phone sends only the digits before the first comma as the destination address digits to the CME or SRST router. Hence, the call proceeds in the manual dialing mode, provided the appropriate dial peer is configured on the router, and users are required to dial out FAC and DTMF digits manually.

For the speed dials where FAC, CMC, and DTMF digits are entered as a continuous string, the phone sends the entire set of digits to CME or SRST router and calls may fail because the CME and SRST router does not have capability to recognize the destination address digits, FAC, and DTMF digits from the digit string received.

### Related Topics

- [Cisco Unified IP Phone setup, on page 537](#)

### BLF speed dial setup

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 with a BLF/SpeedDial button 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 configure only directory numbers as BLF/SpeedDial buttons.

For information on configuring BLF/SpeedDial buttons, see the [Cisco Unified Communications Manager Features and Services Guide](#).

### BLF directed Call Park setup

Directed Call Park allows a user to transfer a parked 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.
For information on configuring BLF/Directed Call Park buttons, see the *Cisco Unified Communications Manager Features and Services Guide*.

## Set up Cisco Unified IP Phone

You can automatically add phones to the Cisco Unified Communications Manager database by using auto-registration or manually add phones by using the Phone Configuration windows.

By enabling auto-registration, you can automatically add a Cisco Unified IP Phone to the Cisco Unified Communications Manager database when you connect the phone to your IP telephony network. During auto-registration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone. In many cases, you might not want to use auto-registration; for example, if you want to assign a specific directory number to a phone.

### Note
Cisco recommends using auto-registration in small configurations or testing labs only.

If you configure the cluster wide security mode to mixed mode, Cisco Unified Communications Manager disables auto-registration.

If you do not use auto-registration, you must manually add phones to the Cisco Unified Communications Manager database.

After you add a Cisco Unified IP Phone to Cisco Unified Communications Manager Administration, the RIS Data Collector service displays the device name, registration status, and the IP address of the Cisco Unified Communications Manager to which the phone is registered in the Phone Configuration window.

Before a Cisco Unified IP Phone can be used, you must use this procedure to add the phone to Cisco Unified Communications Manager. You can also use this procedure to configure third-party phones that are running SIP, H.323 clients, CTI ports, the Cisco ATA 186 Telephone Adaptor, or the Cisco IP Communicator. H.323 clients can comprise Microsoft NetMeeting clients. CTI ports designate virtual devices that Cisco Unified Communications Manager applications such as Cisco SoftPhone and Cisco Unified Communications Manager Auto-Attendant use.

When you add a new phone, you can choose a phone template that was created by the Bulk Administration Tool to configure automatically some of the phone configuration settings, based on the template.

Phone templates must exist on the server before you can select a phone template. For more information about Bulk Administration Tool phone templates, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

### Note
Add the Cisco VG248 and VG224 Phone Ports from the Gateway Configuration window of Cisco Unified Communications Manager Administration.

### Tip
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.
If you plan on using nonstandard phone button and softkey templates, configure the templates before you add the phones.

---

**Procedure**

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

The Find and List Phones window displays.

**Step 2** Perform one of the following tasks:

*Note* You can display the MAC address of a phone.

a) To copy an existing phone, locate the appropriate phone in the Find and List Phones window, click the Copy button next to the phone that you want to copy, and continue with **Step 5**, on page 578.

b) To copy an existing phone and copy the directory numbers, speed dials, busy lamp field/speed dials, and service URLs that are associated with the phone, locate the appropriate phone in the Find and List Phones window, click the Super Copy button next to the phone that you want to copy, and continue with **Step 5**, on page 578.

*Note* The lines that get copied become shared lines between the original phone and the new phone.

c) To add a new phone, click the Add New button and continue with **Step 3**, on page 578.

d) To update an existing phone, locate the appropriate phone and continue with **Step 5**, on page 578.

**Step 3** Perform one of the following tasks when you choose the phone model:

a) From the Phone Type drop-down list box, select the appropriate phone type or device and click Next. After you choose a phone type, you cannot modify it.

b) Select the Phone Template radio button, select the appropriate phone template from the drop-down list box, and click Next. (Only phone templates that were created in the Bulk Administration Tool display in the drop-down list box.)

**Step 4** If the Select the device protocol drop-down list box displays, choose the appropriate protocol of the device and click Next. Otherwise, continue with **Step 5**, on page 578.

The Phone Configuration window displays.

**Step 5** Enter the appropriate settings as described in **Table 89: Phone settings**, on page 541. Only the settings that are appropriate to the chosen phone type display in the window.

**Step 6** Click Save.

If you are adding a phone, a message displays that states that the phone has been added to the database. To add a directory number to this phone, click one of the line links, such as Line [1] - Add a new DN, in the Association Information pane that displays on the left side of the window. Continue to configure the directory number settings.

If you are updating a phone, a message displays that states that you must click the Apply Config button for your changes to take effect and synchronize the phone.

---

**What to Do Next**

You can continue to configure the following on the phone:
• speed-dial buttons
• services
• service URL buttons
• busy lamp field/speed-dial settings

Related Topics
About directory number setup, on page 263
Gateway setup, on page 433
Cisco Unified IP Phone setup, on page 537
BLF speed dial setup, on page 576
Synchronize phone, on page 581
Set up speed-dial buttons or abbreviated dialing, on page 582
Set up IP phone services, on page 583
Display phone MAC address, on page 590
About phone button template setup, on page 671
Create nonstandard softkey templates, on page 676
Add IP phone services to phone buttons, on page 693

Migrate existing phone settings to another phone

The Phone Migration window in Cisco Unified Communications Manager Administration allows you to migrate feature, user, and line configuration for a phone to a different phone. You can migrate data to a different phone model or to the same phone model that runs a different protocol. For example, you can migrate data from a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, or you can migrate data from a phone model that runs SCCP, for example, the Cisco Unified IP Phone 7965 (SCCP) and move it to the same phone model that runs SIP, for example, the Cisco Unified IP Phone 7965 (SIP).

Tip
Phone migration allows you to port existing phone configuration to a new phone without the need to add a phone, lines, speed dials, and so on.

Before you migrate existing phone configuration to a different phone, see the topics related to phone migration for information to review before you migrate the settings and migration procedures.

Before You Begin
Before you can migrate phone configuration to a new phone, consider the following information:

• If the phone models do not support the same functionality, be aware that you may lose functionality on the new phone after the migration occurs. Before you save the migration configuration in the Phone Migration window, Cisco Unified Communications Manager Administration displays a warning that you may lose feature functionality.

• Some phone models do not support phone migration; for example, CTI port, H.323 client, Cisco Unified Mobile Communicator, Cisco IP Softphone, and so on.

• Before you can migrate the phone configuration, you must create a phone template in BAT for the phone model and protocol to which you want to migrate. For example, if you want to migrate the configuration...
for a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, you create the phone template for the Cisco Unified IP Phone 7975.
If the Phone Configuration window does not display a field for the original phone, but the field is required for the new phone, the new phone uses the value from the phone template for the required field.

• The new phone uses the same existing database record as the original phone, so migrating the phone configuration to the new phone removes the configuration for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database; that is, you cannot view or access the configuration for the original phone after the migration. Migrating to a phone that uses fewer speed dials or lines does not remove the speed dials or lines for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database, although some speed dials/lines do not display on the new phone. After you migrate the configuration, you can see all speed dials and lines for the original phone in the Phone Configuration window for the new phone.

• Before you migrate the phone configuration to a new phone, ensure that the phones are unplugged from the network. After you perform the migration tasks, you can plug the new phone into the network and register the device.

• Before you migrate the phone configuration to a new phone, ensure that you have enough device license units for the new phone.

Tip
If you want to migrate the configuration for multiple phones, use the Bulk Administration Tool; for information on how to perform this task, see the Cisco Unified Communications Manager Bulk Administration Guide.

Procedure

Step 1 Make sure that you created a phone template in BAT for the phone model and protocol to which you want to migrate the data. In Cisco Unified Communications Manager Administration, choose Bulk Administration > Phones > Phone Template.

Step 2 In the Find and List Phones window (Device > Phone), find the phone configuration that you want to migrate.

Step 3 After you display the Phone Configuration window for the phone configuration that you want to migrate, choose Migrate Phone from the Related Links drop-down list box.

Step 4 Enter the migration configuration settings, as described in Table 94: Phone migration configuration settings, on page 580.

Step 5 Click Save.

Step 6 If a warning displays that the new phone may lose feature functionality, click OK.

Related Topics

Phone migration settings, on page 580

Phone migration settings

The following table lists configuration settings for phone migration.
### Table 94: Phone migration configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Template</td>
<td>From the drop-down list box, choose the phone template for the phone model to which you want to migrate the phone configuration. Only the phone templates that you configured in the Phone Template window in Bulk Administration display (Bulk Administration &gt; Phones &gt; Phone Template).</td>
</tr>
<tr>
<td>MAC Address</td>
<td>This field support hardware phones only. Enter the Media Access Control (MAC) address for the new Cisco Unified IP Phone to which you are migrating the configuration. Make sure that the value comprises 12 hexadecimal characters. For information on how to access the MAC address for your phone, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model.</td>
</tr>
<tr>
<td>Description</td>
<td>If you want to do so, enter a description for the new phone. The description can include up to 50 characters in any language, but it cannot include double-quotes ('&quot;), percentage sign ('%'), ampersand ('&amp;'), back-slash (''), or angle brackets ('&lt;&gt;').</td>
</tr>
</tbody>
</table>

#### Related Topics

Cisco Unified IP Phone setup, on page 537

### Synchronize phone

To synchronize a phone with the most recent configuration changes, perform the following procedure, which applies 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 Device > Phone. The Find and List Phones window displays.
2. **Step 2** Choose the search criteria to use.
3. **Step 3** Click Find. The window displays a list of phones that match the search criteria.
4. **Step 4** Check the check boxes next to the phones that you want to synchronize. To choose all phones in the window, check the check box in the matching records title bar.
5. **Step 5** Click Apply Config to Selected. The Apply Configuration Information dialog displays.
6. **Step 6** Click OK.
Set up speed-dial buttons or abbreviated dialing

You use Cisco Unified Communications Manager Administration to configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users use Cisco Unified CM User Options to change the speed-dial buttons on their phones.

Table 91: Speed-dial and abbreviated-dial configuration settings, on page 574 describes the speed-dial button and abbreviated dialing configuration settings. The Speed Dial and Abbreviated Dial Configuration window contains the following sections: speed-dial settings on the phone and abbreviated-dial settings that are not associated with a button. The descriptions in Table 91: Speed-dial and abbreviated-dial configuration settings, on page 574 apply to both sections.

The system provides a total of 199 speed-dial and abbreviated-dial settings.

- **Speed Dial Settings**
  Configure these settings for the physical buttons on the phone.

- **Abbreviated Dial Settings**
  Configure these settings for the speed-dial numbers that you access with abbreviated dialing. When the user configures up to 199 speed-dial entries, part of the speed-dial entries can get assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries get used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays on the phone, and the user can access any speed-dial entry by entering the appropriate index (code) for abbreviated dialing.

**Note** Not all Cisco Unified IP Phones support abbreviated dialing. See the phone user guide for information.

**Procedure**

**Step 1** From the Phone Configuration window, choose Add/Update Speed Dials from the Related Links drop-down list box at the top of the window and click Go.

The Speed Dial and Abbreviated Dial Configuration window displays for this phone.

**Note** To display the Phone Configuration window, choose Device > Phone. Enter your search criteria and click Find. Choose the phone for which you want to configure speed-dial buttons.

**Step 2** Enter the appropriate settings as described in Table 91: Speed-dial and abbreviated-dial configuration settings, on page 574.

**Note** For a Pause in Speed Dial, you can enter comma (,) which can act as a delimiter as well as other pause before sending DTMF digits.

**Step 3** To apply the changes, click Save.

**Step 4** To close the window, click Close.
Set up IP phone services

From certain phones, such as Cisco Unified IP Phone 7970, 7960, and 7940, users can access services, such as weather, stock quotes, or other services that are available to them. Using Cisco Unified Communications Manager Administration, you can set up the available services for phones. For some services, users can use the Cisco Unified CM User Options menu to modify the services. For information about the Cisco Unified CM User Options, see the Cisco Unified IP Phone User Guide that is specific to your phone model.

Subscribe to service

You (or an end user) cannot subscribe to services that are marked as enterprise subscriptions. (The enterprise subscription column displays in the Find and List IP Phone Services window. If true displays in the column, you (or an end user) cannot subscribe to the service. In a service is marked as an enterprise subscription, the service automatically displays on the phone, unless you disable the service in the Phone Services Configuration window.

To subscribe to new services for a phone, perform the following steps.

Before You Begin

If you need to do so, add the phone services to Cisco Unified Communications Manager.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Device &gt; Phone. The Find and List Phones window displays.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>To locate a specific phone, enter search criteria and click Find. A list of phones that match the search criteria displays.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the phone to which you want to add a service. The Phone Configuration window displays.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go. The Subscribed IP phone services window displays for this phone.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the Select a Service drop-down list box, choose the service that you want to add to the phone.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Next.</td>
</tr>
</tbody>
</table>
Set up IP phone services

The window displays with the service that you chose. If you want to choose a different service, click Back and repeat Step 5, on page 583.

**Step 7** If the service has required parameters, enter that information into the field that is provided.

**Step 8** Click Subscribe.
   The service displays in the Subscribed Services list.

**Step 9** If you want to subscribe to additional services, click the Subscribe a New Service link in the Subscribed Services area. Repeat Step 5, on page 583 through Step 8, on page 584.

**Related Topics**
   Cisco Unified IP Phone setup, on page 537
   About IP phone service setup, on page 683

**Update service**

Perform the following steps to update a service. You can update the service name and service parameter values, if necessary.

**Procedure**

**Step 1** Choose **Device > Phone**.
   The Find and List Phones window displays.

**Step 2** To locate a specific phone, enter search criteria and click Find.
   A list of phones that match the search criteria displays.

**Step 3** Choose the phone for which you want to update a service.
   The Phone Configuration window displays.

**Step 4** On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go.

**Step 5** From the Subscribed Services list, choose a service.

**Step 6** Update the appropriate parameter and click Save.

**Related Topics**
   Cisco Unified IP Phone setup, on page 537

**Unsubscribe from service**

To unsubscribe from a service, perform the following steps.
Procedure

Step 1  Choose Device > Phone. The Find and List Phones window displays.

Step 2  Enter search criteria to locate a specific phone and click Find. A list of phones that match the search criteria displays.

Step 3  Choose the phone from which you want to delete a service. The Phone Configuration window displays.

Step 4  On the upper, right side of the window, choose Subscribe/Unsubscribe Services from the Related Links drop-down list box and click Go.

Step 5  From the Subscribed Services list, choose a service.

Step 6  Click Unsubscribe. A warning message verifies that you want to unsubscribe from the service.

Step 7  To unsubscribe, click OK or click Cancel to restore your previous settings.

Related Topics
Cisco Unified IP Phone setup, on page 537

Service URL button setup

From some Cisco Unified IP Phone models, users can access information services, such as weather, stock quotes, or other services that are available to them. Using Cisco Unified Communications Manager Administration, you can configure services to be available on a phone button (speed dial button) and then configure that button for the phone. See the Cisco Unified IP Phone User Guide that is specific for your phone model.

Tip
When you configure a service, you specify whether you want the service to display under the Messages, Directory, or Services button. If your phone model has a Messages, Directory, or Services button/option, the service can display under any of these buttons in addition to the phone button for speed dials (service URL button). If a service is marked as an enterprise subscription, you cannot add the service to a service URL button.

Related Topics
IP phone services setup, on page 683

Add service URL button

To configure the service URL buttons for a phone, perform the following steps.
Before You Begin
Before you begin, perform the following configurations:

- Add the services to Cisco Unified Communications Manager.
- Configure the service URL button on the phone button template.
- Subscribe to the service.

Procedure

Step 1  Choose Device > Phone.
The Find and List Phones window displays.

Step 2  To locate a specific phone, enter search criteria and click Find.
A list of phones that match the search criteria displays.

Step 3  Choose the phone to which you want to add a service URL button.
The Phone Configuration window displays.

Step 4  In the Association Information area on the left side of the Phone Configuration window, click the Add a new SURL link.
The Configure Service URL Buttons window displays for this phone.

Step 5  From the Button Service drop-down list box, choose the service that you want to add to or update for the phone.

Step 6  You can change the values in the Label and ASCII Label fields.

Step 7  To add the service to or update for the phone button, click Save.

Step 8  If more buttons and services are available, you can assign additional services to additional buttons by repeating Add service URL button, on page 585 through Add service URL button, on page 585.

Step 9  To close this window and return to the Phone Configuration window, click Close.

Related Topics

Cisco Unified IP Phone setup, on page 537
Set up IP phone services, on page 583
About phone button template setup, on page 671
About IP phone service setup, on page 683

Copy phone record to remote destination profile

You can copy information from a phone record to a new remote destination profile, which is used for Mobile Connect and Mobile Voice Access. See the Cisco Unified Communications Manager Features and Services Guide for instructions on configuring remote destination profiles.
Procedure

Step 1  From the Phone Configuration window, choose Copy to Remote Destination Profile from the Related Links drop-down list box at the top of the window and click Go. The Remote Destination Profile Configuration window displays for this phone.

Step 2  Enter the appropriate settings as described in the topics related to Cisco Unified Mobility in the Cisco Unified Communications Manager Features and Services Guide.

Step 3  To apply the changes, click Save.

Step 4  To close the window, click Close.

Related Topics

Cisco Unified IP Phone setup, on page 537

Modify custom phone button template button items

When you configure a phone and associate it with a custom, nonstandard phone button template, you can modify the phone button items in the associated phone button template. When you do so, you create a new phone button template that is customized for this particular phone. The new phone button template displays in the list of phone button templates with a name of the format "SEP999999999999-Individual Template", where 999999999999 specifies the MAC address of the phone.

Note

You cannot perform this procedure if the phone is associated with a standard phone button template. You must first associate this phone with a custom, nonstandard phone template.

To modify the button items of a custom, nonstandard phone button template, perform the following steps.

Procedure

Step 1  Choose Device > Phone. The Find and List Phones window displays.

Step 2  Enter search criteria and click Find to locate a specific phone. A list of phones that match the search criteria displays.

Step 3  Choose the phone for which you want to modify the phone button items. The Phone Configuration window displays.

Step 4  Click Modify Button Items in the Association Information area on the left side of the window. A popup window warns you that unsaved changes (to the phone) may be lost. If you have made changes to the phone configuration, click Cancel and save those changes before proceeding.

Step 5  Click OK to continue. The Reorder Phone Button Configuration window displays. This window comprises the following panes:
Associated Items
This pane displays a list of the items that are assigned to the phone buttons in this phone button template. The system assigns the first item in the list to button 1, the second item to button 2, and so forth.

Unassigned Associated Items
This pane displays a list of the items that are not assigned to phone buttons in this phone button template.

Dissociate These Items
This pane displays a list of the items that cannot presently be assigned to a phone button.

Step 6 Select an item in the Associated Items pane and click the up or down arrows to change the order of the associated items.
Step 7 Select an item in either the Associated Items or Unassigned Associated Items panes and click the left or right arrows to move the item to the other pane.
Step 8 Select an item in the Associated Items or Unassigned Associated Items panes and click the up or down arrows to move that item to the Dissociate These Items pane or vice versa.
Step 9 Click Save after you have finished moving items among the panes and all items are in the desired order.
Step 10 Click Close to close the Reorder Phone Button Configuration window.

Related Topics
Cisco Unified IP Phone setup, on page 537

Find actively logged-in device

The Cisco Extension Mobility and Cisco Extension Mobility Cross Cluster features keep a record of the devices to which users are actively logged in. For the Cisco Extension Mobility feature, the actively logged-in device report tracks the local phones that are actively logged in by local users; for the Cisco Extension Mobility Cross Cluster feature, the actively logged-in device report tracks the local phones that are actively logged in by remote users.

Cisco Unified Communications Manager provides a specific search window for searching for devices to which users are logged in. Follow these steps to search for a specific device or to list all devices for which users are actively logged in.

Procedure

Step 1 Choose Device > Phone. The Find and List Phones window displays. Records from an active (prior) query may also display in the window.
Step 2 Select the Actively Logged In Device Report from the Related Links drop-down list box in the upper, right corner of the Find and List Phones window and click Go. The Find and List Actively Logged In Devices window displays.
Step 3 To find all actively logged-in device records in the database, ensure the dialog box is empty; go to Step 4, on page 589.
To filter or search records
a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) 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.

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.

Related Topics
Cisco Unified IP Phone setup, on page 537

Find remotely logged-in device

The Cisco Extension Mobility Cross Cluster feature keeps a record of the devices to which users are logged in remotely. The Remotely Logged In Device report tracks the phones that other clusters own but that are actively logged in by local users who are using the EMCC feature.

Cisco Unified Communications Manager provides a specific search window for searching for devices to which users are logged in remotely. Follow these steps to search for a specific device or to list all devices for which users are logged in remotely.

Procedure

Step 1 Choose Device > Phone.
The Find and List Phones window displays. Records from an active (prior) query may also display in the window.

Step 2 Select Remotely Logged In Device from the Related Links drop-down list box in the upper, right corner of the Find and List Phones window and click Go. The Find and List Remotely Logged In Devices window displays.

Step 3 To find all remotely logged-in device records in the database, ensure the dialog box is empty; go to Find actively logged-in device, on page 588.
To filter or search records
a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) 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.

**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.

---

**Related Topics**

Cisco Unified IP Phone setup, on page 537

---

**Display phone MAC address**

The Media Access Control (MAC) address comprises a unique, 12-character, hexadecimal number that identifies a Cisco Unified IP Phone or other hardware device. Locate the number on a label on the bottom of the phone (for example, 000B6A409C405 for Cisco Unified IP Phone 7900 family of phones or SS-00-0B-64-09-C4-05 for Cisco IP Phone SP 12+ and 30 VIP). Cisco Unified Communications Manager makes the MAC address a required field for Cisco Unified IP Phone device configuration. When you enter the MAC address in Cisco Unified Communications Manager fields, do not use spaces or dashes and do not include the "SS" that may precede the MAC address on the label.

For more information on displaying the MAC Address or additional configuration settings on Cisco Unified IP Phones, see the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports the phone model. To display the MAC address for the Cisco IP Phone 12 Series and Cisco IP Phone 30 Series phones or the Cisco VG248 Gateway, perform the following tasks:

- Cisco IP Phone 12 (SP+) Series and 30 Series (VIP)—Press ** to display the MAC address on the second line of the LCD display.

- Cisco VG248 phone ports—The MAC address specifies the endpoint from the Gateway Configuration window of Cisco Unified Communications Manager Administration.

- Cisco VG224 phone ports—You can configure a Cisco VG224 gateway as an MGCP gateway or an SCCP gateway. When it is configured as an SCCP gateway, it can have 24 analog phone endpoints. When it is configured this way, it functions similarly to an IOS SCCP gateway. The MAC address for each individual phone gets calculated by using a formula that considers the slot position, subunit, port, and the last 10 characters of the original MAC address.

- Cisco IP Communicator—Get the MAC address from the network interface of the client PC on which you want to install the Cisco IP Communicator application.

---

**Related Topics**

Gateway setup, on page 433
Trunk setup

This chapter provides information about Cisco Unified Communications Manager trunk configuration.

- About trunk setup, page 591
- Find trunk, page 645
- Set up trunk, page 646
- Delete trunk, page 647
- Reset trunk, page 648
- Synchronize trunk, page 649

About trunk setup

Use a trunk device to configure a logical route to a gatekeeper (that is, the wholesale network or an intercluster trunk with gatekeeper control), to an intercluster trunk without a gatekeeper, or to a SIP network. Choose from the following available trunk types:

- H.225 trunk (gatekeeper controlled)
- Intercluster trunk (gatekeeper controlled)
- Intercluster trunk (non-gatekeeper controlled)
- SIP trunk

Tip

Configure SIP Trunk Security Profiles and SIP Profiles before you configure a SIP Trunk. For more information, see the Cisco Unified Communications Manager Security Guide.
Resetting a trunk drops any calls in progress that are using that trunk. Restarting a gateway tries to preserve the calls in progress that are using that gateway, if possible. Other devices wait until calls complete before restarting or resetting. Resetting/restarting an H.323 or SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager.

For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed. Trunks do not have to undergo a Restart or Reset when Packet Capture is enabled or disabled.

**Related Topics**

- SIP trunk security profile setup, on page 147
- About SIP profile setup, on page 695

**H.225 and intercluster trunks settings**

The following table describes the trunk settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks.

<table>
<thead>
<tr>
<th>Table 95: H.225 and intercluster trunks settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Device Information</td>
</tr>
<tr>
<td>Device Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td><strong>Note</strong></td>
</tr>
</tbody>
</table>
Choosethecommondeviceconfigurationtowhichyouwantthistrunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window.

**Call Classification**

This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet).

When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet.

This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. The alerting tones are provided by Cisco Unified Communications Manager Annunciators.

Use this parameter in conjunction with the settings on the Route Pattern Configuration window to classify an outgoing call as OnNet or OffNet.

**Media Resource Group List**

This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines.

**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 trunk.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this trunk consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the System Location menu option.

For an explanation of location-based CAC across intercluster trunks, see the Cisco Unified Communications Manager System Guide.

The location also associates with the RSVP policy with regard to other locations. The configuration allows RSVP to be enabled and disabled based upon location pairs.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR Group</td>
<td>Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.</td>
</tr>
<tr>
<td>Tunneled Protocol</td>
<td>This drop-down list box displays for H.225 trunks, gatekeeper-controlled trunks, and non-gatekeeper-controlled trunks. Choose the QSIG option if you want to use trunks to transport (tunnel) non-H.323 protocol information in H.323 signaling messages from Cisco Unified Communications Manager to other Annex M.1-compliant H.323 PINXs. QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, and Message Waiting Indication.</td>
</tr>
</tbody>
</table>
| QSIG Variant | To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the drop-down list box, choose one of the following options:  
  • No Changes—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise.  
  • Not Selected  
  • ECMA—Choose for ECMA PBXs that use Protocol Profile 0x91.  
  • ISO—Choose for PBXs that use Protocol Profile 0x9F.  
For more information, see the following information:  
  • Be aware that the QSIG Variant can also be defined as a clusterwide parameter.  
  • For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN.1 ROSE OID Encoding</td>
<td>To display the options in the ASN.1 ROSE OID Encoding drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• No Changes—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise.</td>
</tr>
<tr>
<td></td>
<td>• Not Selected</td>
</tr>
<tr>
<td></td>
<td>• Use Global Value ECMA—If you chose the ECMA option from the QSIG Variant drop-down list box, choose this option.</td>
</tr>
<tr>
<td></td>
<td>• Use Global Value ISO—If you chose the ISO option from the QSIG Variant drop-down list box, choose this option.</td>
</tr>
<tr>
<td></td>
<td>• Use Local Value</td>
</tr>
</tbody>
</table>

For more information, see the following information:

• Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide parameter.

• For information on QSIG support with Cisco Unified Communications Manager, see the *Cisco Unified Communications Manager System Guide*. 
### Packet Capture Mode

This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions.

Choose one of the following options from the drop-down list box:

- **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting.

- **Batch Processing Mode**—Cisco Unified Communications Manager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified Communications Manager stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The IREC tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.

**Tip** You do not have to reset the trunk after enabling/disabling Packet Capturing.

For more information on capturing packets, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

### Packet Capture Duration

This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions.

This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes.

To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.

For more information on capturing packets, see the *Cisco Unified Communications Manager Troubleshooting Guide*. 
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Termination Point Required</td>
<td>This check box is used to indicate whether a media termination point (MTP) is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use a media termination point to implement features. Uncheck the Media Termination Point Required check box if you do not want to use a media termination point to implement features. Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 Empty Capabilities Set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and one or both parties are a video endpoint, the call operates as audio only.</td>
</tr>
<tr>
<td>Retry Video Call as Audio</td>
<td>This check box applies only to video endpoints that receive a call. For trunks, this check box pertains to calls that are received from Cisco Unified Communications Manager but not to calls that are received from the wide-area network (WAN). By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and/or route/hunt list.</td>
</tr>
<tr>
<td>Wait for Far-End H.245 Terminal Capability Set</td>
<td>This field applies only to H.323 devices. This check box specifies that Cisco Unified Communications Manager waits to receive the far-end H.245 Terminal Capability Set before it sends its H.245 Terminal Capability Set. By default, the system checks this check box. To specify that Cisco Unified Communications Manager should initiate capabilities exchange, uncheck this check box.</td>
</tr>
<tr>
<td>Path Replacement Support</td>
<td>If you choose the QSIG option from the Tunneled Protocol drop-down list box, this check box displays for H.225 trunks, gatekeeper-controlled trunks, and non-gatekeeper-controlled trunks. This setting works with QSIG tunneling (Annex M.1) to ensure that non-H.323 information gets sent on the leg of the call that uses path replacement. Note: The default setting leaves the check box unchecked. When you choose the QSIG Tunneled Protocol option, the system automatically checks the check box.</td>
</tr>
</tbody>
</table>
### Field Description

**Transmit UTF-8 for Calling Party Name**

This device uses the user locale setting of the SIP trunks to determine whether to send unicode and whether to translate received Unicode information.

For the sending device, if you check this check box and the user locale setting in the device pool at the device matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII.

The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool of the device. If the user locale setting matches the terminating phone user locale, the phone displays the characters.

*Note*  The phone may display garbled characters if the two ends of the trunk configure user locales that do not belong to the same language group.

**Unattended Port**

Check this check box if calls can be redirected, transferred and forwarded to an unattended port, such as a voice mail port.

The default value for this check box leaves it unchecked.

**SRTP Allowed**

Check the SRTP Allowed check box if you want Cisco Unified Communications Manager to allow secure and nonsecure calls over the trunk.

If you do not check this check box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP.

*Caution*  If you check this check box, Cisco strongly recommends that you configure IPSec, so you do not expose keys and other security-related information during call negotiations. If you do not configure IPSec correctly, consider signaling between Cisco Unified Communications Manager and the gateway as nonsecure.

For more information on encryption for trunks, see the *Cisco Unified Communications Manager Security Guide*.

**H.235 Pass Through Allowed**

This feature allows Cisco Unified Communications Manager to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel.

To allow H.235 pass through, check the check box.
**Enable SAF**

Check this check box if you want to enable this intercluster (non-gatekeeper controlled) trunk for SAF.

When a trunk is enabled for SAF, the trunk can support the call control discovery feature. SAF-enabled trunks that are assigned to the CCD advertising service in the Advertising Service window handle inbound calls from remote call-control entities that use the SAF network. *(Call Routing > Call Control Discovery > Advertising Service)*

SAF-enabled trunks that are assigned to the CCD requesting service handle outgoing calls to learned patterns. *(Call Routing > Call Control Discovery > Requesting Service)*

For more information on the call control discovery feature, see the Cisco Unified Communications Manager Features and Services Guide.

**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:

- **Default**—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.

- **Off**—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

- **On**—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

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 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 Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.
If you use the Cisco Intercompany Media Engine feature, check this checkbox to indicate that calls made through this trunk might reach the PSTN. Check this checkbox even if all calls through this trunk device do not reach the PSTN. For example, check this checkbox for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN.

When checked, this checkbox causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. By default, this checkbox remains checked.

For more information on Cisco Intercompany Media Engine, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

### Intercompany Media Engine (IME)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSTN Access</td>
<td>If you use the Cisco Intercompany Media Engine feature, check this checkbox</td>
</tr>
<tr>
<td></td>
<td>to indicate that calls made through this trunk might reach the PSTN. Check</td>
</tr>
<tr>
<td></td>
<td>this checkbox to indicate that calls made through this trunk might reach the</td>
</tr>
<tr>
<td></td>
<td>PSTN. Check this checkbox even if all calls through this trunk device do</td>
</tr>
<tr>
<td></td>
<td>not reach the PSTN. For example, check this checkbox for tandem trunks or</td>
</tr>
<tr>
<td></td>
<td>an H.323 gatekeeper routed trunk if calls might go to the PSTN. When</td>
</tr>
<tr>
<td></td>
<td>checked, this checkbox causes the system to create upload voice call</td>
</tr>
<tr>
<td></td>
<td>records (VCRs) to validate calls made through this trunk device. By</td>
</tr>
<tr>
<td></td>
<td>default, this checkbox remains checked.</td>
</tr>
<tr>
<td></td>
<td>For more information on Cisco Intercompany Media Engine, see the</td>
</tr>
<tr>
<td></td>
<td><em>Cisco Intercompany Media Engine Installation and Configuration Guide</em>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.164 Transformation Profile</td>
<td>Check this checkbox if you want to use the Cisco Intercompany Media Engine</td>
</tr>
<tr>
<td></td>
<td>and calls might reach the PSTN. For more information, see the *Cisco</td>
</tr>
<tr>
<td></td>
<td>Intercompany Media Engine Installation and Configuration Guide*.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, choose the appropriate E.164 transformation</td>
</tr>
<tr>
<td></td>
<td>that you created on the Intercompany Media Services E.164 Transformation</td>
</tr>
<tr>
<td></td>
<td>Configuration window (Advanced Features &gt; Intercompany Media Services &gt; E.164</td>
</tr>
<tr>
<td></td>
<td>Transformation). For more information on Cisco Intercompany Media Engine,</td>
</tr>
<tr>
<td></td>
<td>see the *Cisco Intercompany Media Engine Installation and Configuration</td>
</tr>
<tr>
<td></td>
<td>Guide*.</td>
</tr>
</tbody>
</table>

### Incoming Calling Party Settings

<table>
<thead>
<tr>
<th>Field</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 Clear</td>
</tr>
<tr>
<td></td>
<td>Prefix Setting.</td>
</tr>
<tr>
<td>Default Prefix Setting</td>
<td>To enter the default value for all prefix fields at the same time, click</td>
</tr>
<tr>
<td></td>
<td>Default Prefix Settings.</td>
</tr>
</tbody>
</table>

**Cisco Unified Communications Manager Administration Guide, Release 9.1(1)**

600

OL-27945-01
Configure the following settings to globalize calling party numbers that use National 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 National for the Calling Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix.
  
  If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of National type before it applies the prefixes.

- **Use Device Pool CSS**—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.

- **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.

  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.

**Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*. 

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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—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. 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>
<tr>
<td>Tip</td>
<td>For more information on configuring these settings, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>
Configure the following settings to globalize calling party numbers that use International for the Calling Party Number Type.

<table>
<thead>
<tr>
<th>Field</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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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—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. 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>

**Tip**  
For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*. 
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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).
  
  If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes.

- **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.

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.

**Tip** For more information on configuring these settings, see the Cisco Unified Communications Manager Features and Services Guide.

### Field Description

<table>
<thead>
<tr>
<th>Field</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>
</tbody>
</table>

- **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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#).

  If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes.

- **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.

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.

**Tip** For more information on configuring these settings, see the Cisco Unified Communications Manager Features and Services Guide.
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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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**—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.

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.

**Tip**  For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

### Incoming Called Party Settings

The H.323 protocol does not support the international escape character +. To ensure the correct prefixes, including the +, get applied to inbound calls over H.323 trunks, configure the incoming called party settings; that is, configuring the incoming called party settings ensures that when an inbound call comes from a H.323 trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk.

<table>
<thead>
<tr>
<th>Field</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>- <strong>Prefix</strong>—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 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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>Strip Digits</strong>—Enter the number of digits, up to the number 24, 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>- <strong>Use Device Pool CSS</strong>—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>- <strong>Calling Search Space</strong>—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. 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>

**Tip**  For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

### Clear Prefix Settings

To delete all prefixes for all called party number types, click Clear Prefix Settings.
To enter the default value for all prefix fields at the same time, click Default Prefix Settings.

Configure the following settings to transform incoming called party numbers that use National for the Called Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use National for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called 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 called party number of National type before it applies the prefixes.

- **Use Device Pool CSS**—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.

- **Calling Search Space**—This setting allows you to transform the called party number of National called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality.

  **Tip** To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field.

- **Strip Digits**—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes.

- **Use Device Pool CSS**—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.

- **Calling Search Space**—This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Number</td>
<td>Configure the following settings to transform incoming called party numbers that use International for the Called Party Number Type.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Cisco Unified Communications Manager applies the prefix that you enter in this field to called party numbers that use International for the Called Party Numbering Type. You can enter up to 16 characters, which include digits, the international escape character (+), asterisk (*), or the pound sign (#). You can enter the word, Default, instead of entering a prefix. If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality. <strong>Tip</strong> To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field.</td>
</tr>
<tr>
<td>Strip Digits</td>
<td>Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of International type before it applies the prefixes.</td>
</tr>
<tr>
<td>Use Device Pool CSS</td>
<td>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>Calling Search Space</td>
<td>This setting allows you to transform the called party number of International called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.</td>
</tr>
</tbody>
</table>
Configure the following settings to transform incoming called party numbers that use Unknown for the Called Party Number Type.

- **Prefix** — Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Unknown for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality.

  **Tip** To configure the Strip Digits field, 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.

- **Strip Digits** — Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Unknown type before it applies the prefixes.

- **Use Device Pool CSS** — 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 transform the called party number of Unknown called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.
Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type.

- **Prefix**—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 called party prefix, which supports both the prefix and strip digit functionality.

  **Tip**  To configure the Strip Digits field, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, do not enter the word, Default, in the Prefix field.

- **Strip Digits**—Enter the number of digits that you want Cisco Unified Communications Manager to strip from the called party number of Subscriber type before it applies the prefixes.

- **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 transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.

### Multilevel Precedence and Preemption (MLPP) Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber Number</td>
<td>Configure the following settings to transform incoming called party numbers that use Subscriber for the Called Party Number Type.</td>
</tr>
<tr>
<td></td>
<td>- Prefix—Cisco Unified Communications Manager applies the prefix that you enter in this field to called numbers that use Subscriber for the Called Party Numbering Type. You can enter up to 16 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, you cannot configure the Strip Digits field. 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 thePrefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming called 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, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields, 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 called party number of Subscriber type before it applies the prefixes.</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 transform the called party number of Subscriber called party number type on the device. If you choose None, no transformation occurs for the incoming called party number. Make sure that the calling search space that you choose contains the called party transformation pattern that you want to assign to this device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Domain</td>
<td>From the drop-down list box, choose an MLPP domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that was set for the device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that was set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
</tbody>
</table>
If available, this setting specifies whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting to assign to this device from the following options:

- **Default**—This device inherits its MLPP indication setting from its device pool.
- **Off**—This device does not handle nor process indication of an MLPP precedence call.
- **On**—This device does handle and process indication of an MLPP precedence call.

**Note** Do not configure a device with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

### Call Routing Information

#### Inbound Calls

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Significant Digits</strong></td>
<td>Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the H.323 device. Choose the number of significant digits to collect, from 0 to 32. Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called.</td>
</tr>
</tbody>
</table>

| **Calling Search Space** | From the drop-down list box, select the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number. You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 Spaces window. **Note** To set the maximum list box items, choose **System > Enterprise Parameters** and choose CCMAdmin Parameters. |

| **AAR Calling Search Space** | Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. |
Enter the prefix digits that are appended to the called party number on incoming calls.
Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +.

Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco Unified Communications Manager. (The UUIE part of the SETUP message includes the Redirecting Number IE.)
Uncheck the check box to exclude the Redirecting Number IE.
You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.

Default leaves the check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.

Check this check box to enable the H.323 FastStart call connections on incoming calls.
By default, the check box remains unchecked for the H.323 gateway.
For intercluster calls, you must check the Enable Inbound FastStart check box on Cisco Unified Communications Manager servers in other clusters for the outbound FastStart feature to work.

To use the Called 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 Called Party Transformation CSS that you configured for this device in the Trunk Configuration window.

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 Trunk Configuration window.
### Calling Party Selection
Choose the directory number that is sent on an outbound call on a gateway.

The following options specify which directory number is sent:

- **Originator**—Send the directory number of the calling device.
- **First Redirect Number**—Send the directory number of the redirecting device.
- **Last Redirect Number**—Send the directory number of the last device to redirect the call.
- **First Redirect Number (External)**—Send the external directory number of the redirecting device.
- **Last Redirect Number (External)**—Send the external directory number of the last device to redirect the call.

### Calling Line ID Presentation
Cisco Unified Communications Manager uses calling line ID presentation (CLIP) as a supplementary service to control the display of the calling party number on the called party phone display screen.

Choose Default if you do not want to change the presentation setting. Choose Allowed if you want calling number information to display. Choose Restricted if you do not want the calling number information to display.

### Called Party IE Number Type
Choose the format for the type of number in called party directory numbers.

Cisco Unified Communications Manager sets the called 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 called directory number to be encoded to a non-national numbering plan type.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Cisco Unified Communications Manager sets the directory number type.
- **Unknown**—This option indicates that 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.
### Field | Description
--- | ---
Calling Party IE Number Type Unknown | Choose the format for the type of number 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 Unified Communications Manager**—Cisco Unified Communications Manager sets the directory number type.
- **Unknown**—This option indicates that 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.

**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 Cisco Unified Communications Manager, which is the default, your configuration for this field overwrites the Calling Party Number Type setting for the outgoing call through a particular gateway.
### Called Numbering Plan

Choose the format for the numbering plan in called party directory numbers.

Cisco Unified Communications Manager sets the called DN numbering plan. 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 called numbering plan to be encoded to a non-national numbering plan.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—This option indicates that the dialing plan is unknown.

### Calling Numbering Plan

Choose the format for the numbering plan in calling party directory numbers.

Cisco Unified Communications Manager sets the calling DN numbering plan. 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 numbering plan to be encoded to a non-national numbering plan.

Choose one of the following options:

- **Cisco Unified Communications Manager**—Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN**—Use when you are dialing outside the dialing plan for your country.
- **National Standard**—Use when you are dialing within the dialing plan for your country.
- **Private**—Use when you are dialing within a private network.
- **Unknown**—This option indicates that the dialing plan is unknown.
**Field** | **Description**  
--- | ---  
Caller ID DN | Enter the pattern, from 0 to 24 digits, that you want to use to format the caller ID on outbound calls from the trunk.  
For example, in North America  
- 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it.  
- 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.  
You can enter the international escape character +.  

Display IE Delivery | Check this check box to enable delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service.  
**Note** The default setting leaves this check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.  

Redirecting Number IE Delivery - Outbound | Check this check box to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded. (The UUIE part of the outgoing SETUP message from the Cisco Unified Communications Manager includes the Redirecting Number IE.)  
Uncheck the check box to exclude the first Redirecting Number and the redirecting reason.  
You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.  
**Note** The default setting leaves this check box checked. You cannot check this check box if you choose the QSIG option from the Tunneled Protocol drop-down list box.  

Enable Outbound FastStart | Check this check box to enable the H.323 FastStart feature on outgoing calls.  
By default, the check box remains unchecked for the H.323 gateway or trunk.  
When you check the Enable Outbound FastStart check box, you must set the Media Termination Point Required, Media Resource Group Lists, and Codec for Outbound FastStart.
ChoosethecodecforusewiththeH.323deviceforanoutbound
FastStartcall:
• G711 mu-law 64K (default)
• G711 a-law 64K
• G723
• G729
• G729AnnexA
• G729AnnexB
• G729AnnexA-AnnexB

When you check the Enable Outbound FastStart check box, you must
choose the codec for supporting outbound FastStart calls.

Gatekeeper Information
(for gatekeeper-controlled H.225 trunks and intercluster trunks)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Codec For Outbound FastStart | Choose the codec for use with the H.323 device for an outbound FastStart call:  
  • G711 mu-law 64K (default)  
  • G711 a-law 64K  
  • G723  
  • G729  
  • G729AnnexA  
  • G729AnnexB  
  • G729AnnexA-AnnexB  

<table>
<thead>
<tr>
<th>Gatekeeper Name</th>
<th>Choose the gatekeeper that controls this trunk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>For a gatekeeper-controlled trunk to register correctly with a gatekeeper through use of H.323 dynamic addressing, you must set the Send Product ID and Version ID service parameter to True. (The default value specifies False.) To do so, choose System &gt; Service Parameters and find the Send Product ID and Version ID service parameter for the Cisco CallManager service in the Clusterwide Parameters (Device - H323) portion of the Service Parameter Configuration window.</td>
</tr>
</tbody>
</table>

| Terminal Type       | Use the Terminal Type field to designate the type for all devices that this trunk controls.  
  Always set this field to Gateway for normal trunk call admission control. |

Cisco Unified Communications Manager Administration Guide, Release 9.1(1)
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Technology Prefix | Use this optional field to eliminate the need for entering the IP address of every Cisco Unified Communications Manager when configuring the gw-type-prefix on the gatekeeper:  
  - If you leave this field blank (the default setting), you must specify the IP address of each Cisco Unified Communications Manager that can register with the gatekeeper when you enter the gw-type-prefix command on the gatekeeper.  
  - When you use this field, make sure that the value that you enter exactly matches the type-prefix value that is specified with the gw-type-prefix command on the gatekeeper.  

For example, if you leave this field blank and you have two Cisco Unified Communications Managers with IP addresses of 10.1.1.2 and 11.1.1.3, enter the following gw-type-prefix command on the gatekeeper:  
gw-type-prefix 1## default-technology gw ip 10.1.1.2 gw ip 11.1.1.3  
If you enter 1## in this field, enter the following gw-type-prefix command on the gatekeeper:  
gw-type-prefix 1## default-technology |
| Zone | Use this optional field to request a specific zone on the gatekeeper with which Cisco Unified Communications Manager will register. The zone specifies the total bandwidth that is available for calls between this zone and another zone:  
  - If you do not enter a value in this field, the zone subnet command on the gatekeeper determines the zone with which Cisco Unified Communications Manager registers. Cisco recommends the default setting for most configurations.  
  - If you want Cisco Unified Communications Manager to register with a specific zone on the gatekeeper, enter the value in this field that exactly matches the zone name that is configured on the gatekeeper with the zone command. Specifying a zone name in this field eliminates the need for a zone subnet command for each Cisco Unified Communications Manager that is registered with the gatekeeper.  

See the command reference documentation for your gatekeeper for more information. |
| Remote Cisco Unified Communications Manager Information  
(for non-gatekeeper-controlled intercluster trunks) |  |
| Server 1 IP Address/Host Name | Enter the IP address or host name of the first remote Cisco Unified Communications Manager that this trunk accesses. |
### Field | Description
--- | ---
Server 2 IP Address/Host Name | Enter the IP address or host name of the second remote Cisco Unified Communications Manager that this trunk accesses.  
**Note** If this non-gatekeeper-controlled intercluster trunk accesses the device pool of a remote non-gatekeeper-controlled intercluster trunk and that device pool has a second Cisco Unified Communications Manager node, you must enter the second remote Cisco Unified Communications Manager IP address/host name in this field.

Server 3 IP Address/Host Name | Enter the IP address or host name of the third remote Cisco Unified Communications Manager that this trunk accesses.  
**Note** If this non-gatekeeper-controlled intercluster trunk accesses the device pool of a remote non-gatekeeper-controlled intercluster trunk and that device pool has a third Cisco Unified Communications Manager node, you must enter the third remote Cisco Unified Communications Manager IP address/host name in this field.

#### UIIE Configuration

**Passing Precedence Level Through UIIE** | Check this check box to enable passing MLPP information through the PRI 4ESS UIIE field. The system uses this box for interworking with DRSN switch.  
The system makes this check box available only if the PRI Protocol Type value of PRI 4ESS is specified for this trunk.  
The default value specifies unchecked.

**Security Access Level** | Enter the value for the security access level. Valid values include 00 through 99. The system makes this field available only if the Passing Precedence Level Through UIIE check box is checked. The default value specifies 2.

#### Geolocation Configuration

**Geolocation** | From the drop-down list box, choose a geolocation.  
You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.  
You can also choose a geolocation that has been configured with the **System > Geolocation Configuration** menu option.  
For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.  
For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.  

From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device.

You can also choose a geolocation filter that has been configured with the System > Geolocation Filter menu option.

For an explanation of geolocation filters, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide.

For an overview and details of how logical partitioning uses geolocation filters, see the Cisco Unified Communications Manager Features and Services Guide.

**Send Geolocation Information**

Check this box to send geolocation information for this device.

For an overview and details of how logical partitioning uses geolocation information, see the Cisco Unified Communications Manager Features and Services Guide.

---

**Related Topics**

- Location setup, on page 107
- Service parameter setup, on page 131
- About calling search space setup, on page 247

---

**SIP trunk settings**

The following table describes the settings for SIP trunks.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geolocation Filter</td>
<td>From the drop-down list box, choose a geolocation filter. If you leave the &lt;None&gt; setting, no geolocation filter gets applied for this device. You can also choose a geolocation filter that has been configured with the System &gt; Geolocation Filter menu option. For an explanation of geolocation filters, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide. For an overview and details of how logical partitioning uses geolocation filters, see the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td>Send Geolocation Information</td>
<td>Check this box to send geolocation information for this device. For an overview and details of how logical partitioning uses geolocation information, see the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
</tbody>
</table>
### Table 96: SIP trunk settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trunk Service Type</td>
<td>Choose one of the following options from the Trunk Service Type drop-down list box:</td>
</tr>
<tr>
<td></td>
<td>• None—Choose this option if the trunk will not be used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine.</td>
</tr>
<tr>
<td></td>
<td>• Call Control Discovery—Choosing this option enables the trunk to support call control discovery. If you assign this trunk to the CCD advertising service in the Advertising Service window, the trunk handles inbound calls from remote call-control entities that use the SAF network. If you assign this trunk to the CCD requesting service in the Requesting Service window, the trunk handles outgoing calls to learned patterns. For more information on the call control discovery feature, see the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td></td>
<td>• Extension Mobility Cross Cluster—Choose this option to enable the trunk to support the Extension Mobility Cross Cluster (EMCC) feature. Choosing this option causes the following settings to remain blank or unchecked and become unavailable for configuration, thus retaining their default values: Media Termination Point Required, Unattended Port, Destination Address, Destination Address IPv6, and Destination Address is an SRV. For more information about the EMCC feature, see the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Intercompany Media Engine—Ensure that the Cisco IME server is installed and available before you configure this field.</td>
</tr>
<tr>
<td>Tip</td>
<td>After you choose Call Control Discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine for the trunk service type and click Next, you cannot change the trunk to a different type.</td>
</tr>
</tbody>
</table>

### Device Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter a unique identifier for the trunk. Enter a unique identifier for the trunk. The device name can include up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the trunk. The description can include up to 114 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Device Pool | Choose the appropriate device pool for the trunk. For trunks, device pools specify a list of Cisco Unified Communications Managers that the trunk uses to distribute the call load dynamically. **Note** Calls that are initiated from a phone that is registered to a Cisco Unified Communications Manager that does not belong to the device pool of the trunk use different Cisco Unified Communications Managers of this device pool for different outgoing calls. Selection of Cisco Unified Communications Manager nodes occurs in a random order. A call that is initiated from a phone that is registered to a Cisco Unified Communications Manager that does belong to the device pool of the trunk uses the same Cisco Unified Communications Manager node for outgoing calls if the Cisco Unified Communications Manager is up and running. The default value for Device Pool specifies Not Selected.

Common Device Configuration | Choose the common device configuration to which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window.

Call Classification | This parameter determines whether an incoming call through this trunk is considered off the network (OffNet) or on the network (OnNet). The default value for Call Classification is Use System Default. When the Call Classification field is configured as Use System Default, the setting of the Cisco Unified Communications Manager clusterwide service parameter, Call Classification, determines whether the trunk is OnNet or OffNet. This field provides an OnNet or OffNet alerting tone when the call is OnNet or OffNet, respectively. Use this parameter in conjunction with the settings on the Route Pattern Configuration window to classify an outgoing call as OnNet or OffNet.

Media Resource Group List | This list provides a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from among the available media resources according to the priority order that a Media Resource Group List defines. The default value for Media Resource Group List specifies None.
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 trunk.

A location setting of Hub_None means that the locations feature does not keep track of the bandwidth that this trunk consumes. A location setting of Phantom specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.

To configure a new location, use the **System > Location** menu option.

For an explanation of location-based CAC across intercluster trunks, see the *Cisco Unified Communications Manager System Guide*.

The location also associates with the RSVP policy with regard to other locations. The configuration allows RSVP to be enabled and disabled based upon location pairs.

Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted.

The default value for AAR Group specifies None.

Select the QSIG option if you want to use SIP trunks or SIP gateways to transport (tunnel) QSIG messages from Cisco Unified Communications Manager to other PINXs. QSIG tunneling supports the following features: Call Back, Call Completion, Call Diversion, Call Transfer, Identification Services, Path Replacement, and Message Waiting Indication (MWI).

**Note** Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the R PID headers on the SIP gateway.

To turn off R PID headers on the SIP gateway, apply a SIP profile to the voIP dial peer on the gateway, as shown in the following example:

```
voice class sip-profiles 1000 request ANY sip-header Remote-Party_ID remove
response ANY sip-header Remote-Party-ID remove

dial-peer voice 124 voip
destination-pattern 3...
signaling forward unconditional
session protocol sipv2
session target ipv4:<ip address>
voice-class sip profiles 1000
```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QSIG Variant</td>
<td>To display the options in the QSIG Variant drop-down list box, select QSIG</td>
</tr>
<tr>
<td></td>
<td>from the Tunneled Protocol drop-down list box.</td>
</tr>
<tr>
<td></td>
<td>This parameter specifies the protocol profile that is sent in outbound</td>
</tr>
<tr>
<td></td>
<td>QSIG facility information elements.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• No Changes—Default. Keep this parameter set to the default value</td>
</tr>
<tr>
<td></td>
<td>unless a Cisco support engineer instructs otherwise.</td>
</tr>
<tr>
<td></td>
<td>• Not Selected</td>
</tr>
<tr>
<td></td>
<td>• ECMA—Select for ECMA PBX systems that use Protocol Profile 0x91.</td>
</tr>
<tr>
<td></td>
<td>• ISO—Select for PBX systems that use Protocol Profile 0x9F.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the following information:</td>
</tr>
<tr>
<td></td>
<td>• Be aware that the QSIG Variant can also be defined as a clusterwide</td>
</tr>
<tr>
<td></td>
<td>parameter.</td>
</tr>
<tr>
<td></td>
<td>• For information on QSIG support with Cisco Unified Communications Manager,</td>
</tr>
<tr>
<td></td>
<td>see the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN.1 ROSE OID Encoding</td>
<td>To display the options in the ASN.1 ROSE OID Encoding drop-down list box,</td>
</tr>
<tr>
<td></td>
<td>choose QSIG from the Tunneled Protocol drop-down list box.</td>
</tr>
<tr>
<td></td>
<td>This parameter specifies how to encode the Invoke Object ID (OID) for</td>
</tr>
<tr>
<td></td>
<td>remote operations service element (ROSE) operations.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• No Changes—Default. Keep this parameter set to the default value</td>
</tr>
<tr>
<td></td>
<td>unless a Cisco support engineer instructs otherwise.</td>
</tr>
<tr>
<td></td>
<td>• Not Selected</td>
</tr>
<tr>
<td></td>
<td>• Use Global Value ECMA—If you selected the ECMA option from the QSIG</td>
</tr>
<tr>
<td></td>
<td>Variant drop-down list box, select this option.</td>
</tr>
<tr>
<td></td>
<td>• Use Global Value ISO—If you selected the ISO option from the QSIG</td>
</tr>
<tr>
<td></td>
<td>Variant drop-down list box, select this option.</td>
</tr>
<tr>
<td></td>
<td>• Use Local Value</td>
</tr>
<tr>
<td></td>
<td>For more information, see the following information:</td>
</tr>
<tr>
<td></td>
<td>• Be aware that ASN.1 ROSE OID Encoding can also be defined as a clusterwide</td>
</tr>
<tr>
<td></td>
<td>parameter.</td>
</tr>
<tr>
<td></td>
<td>• For information on QSIG support with Cisco Unified Communications Manager,</td>
</tr>
<tr>
<td></td>
<td>see the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Packet Capture Mode | This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions.

Choose one of the following options from the drop-down list box:

- **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting.

- **Batch Processing Mode**—Cisco Unified Communications Manager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified Communications Manager stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.

Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices.

For more information on capturing packets, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

Packet Capture Duration | This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions.

This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes.

To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.

For more information on capturing packets, see the *Cisco Unified Communications Manager Troubleshooting Guide*. 

### Field | Description
--- | ---
Media Termination Point Required | You can configure Cisco Unified Communications Manager SIP trunks to always use an MTP. Check this check box to provide media channel information in the outgoing INVITE request. When this check box is checked, all media channels must terminate and reoriginate on the MTP device. If you uncheck the check box, the Cisco Unified Communications Manager can decide whether calls are to go through the MTP device or be connected directly between the endpoints.  
**Note**  
If check box remains unchecked (default case), Cisco Unified Communications Manager will attempt to dynamically allocate an MTP if the DTMF methods for the call legs are not compatible.  
For example, existing phones that run SCCP support only out-of-band DTMF, and existing phones that run SIP support RFC2833. Because the DTMF methods are not identical, the Cisco Unified Communications Manager dynamically allocates an MTP. If, however, a new phone that runs SCCP, which supports RFC2833 and out-of-band, calls an existing phone that runs SIP, Cisco Unified Communications Manager does not allocate an MTP because both phones support RFC2833. So, by having the same type of DTMF method supported on each phone, no need exists for MTP.

Retry Video Call as Audio | This check box pertains to outgoing SIP trunk calls and does not impact incoming calls.  
By default, the system checks this check box to specify that this device should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting.  
If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR) and/or route/hunt list.

Path Replacement Support | This check box displays when you select QSIG from the Tunneled Protocol drop-down list box. This setting works with QSIG tunneling to ensure that non-SIP information gets sent on the leg of the call that uses path replacement.  
**Note**  
The default setting leaves the check box unchecked. When you select the QSIG Tunneled Protocol option, the system automatically checks the check box. Alternatively, if the Tunneled Protocol option is set to None, the Path Replacement Support check box displays as grayed out and is not available.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Transmit UTF-8 for Calling Party Name | This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information.  
For the sending device, if you check this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode. If the user locale settings do not match, the device sends ASCII.  
The receiving device translates incoming unicode characters based on the user locale setting of the sending device pool. If the user locale setting matches the terminating phone user locale, the phone displays the characters.  
**Note**  
The phone may display malformed characters if the two ends of the trunk configure user locales that do not belong to the same language group.  
The default value for Transmit UTF-8 for Calling Party Name leaves the check box unchecked. |
| Transmit UTF-8 Names in QSIG APDU | This device uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information.  
For the sending device, if you check this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode and encodes in UTF-8 format. If the user locale settings do not match, the device sends ASCII and encodes in UTF-8 format.  
If the configuration parameter is not set and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode (if the name uses 8-bit format) and encodes in ISO8859-1 format.  
The default value for Transmit UTF-8 Names in QSIG APDU leaves the check box unchecked. |
| Unattended Port | Check this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port.  
The default value for this check box leaves it unchecked. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRTP Allowed</td>
<td>Check this check box if you want Cisco Unified Communications Manager to allow secure and nonsecure media calls over the trunk. Checking this check box enables Secure Real-Time Protocol (SRTP) SIP Trunk connections and also allows the SIP trunk to fall back to Real-Time Protocol (RTP) if the endpoints do not support SRTP. If you do not check this box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP negotiation instead. The default value for this check box leaves it unchecked. <strong>Caution</strong> If you check this check box, Cisco strongly recommends that you use an encrypted TLS profile, so that keys and other security-related information do not get exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will get exposed in signaling and traces. In that case, you must ensure the security of the network between Cisco Unified Communications Manager and the destination side of the trunk. For more information on encryption for trunks, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
</tbody>
</table>
| Consider Traffic on This Trunk Secure | This field provides an extension to the existing security configuration on the SIP trunk, which enables a SIP trunk call leg to be considered secure if SRTP is negotiated, independent of the signaling transport. Choose one of the following values:  
• When using both sRTP and TLS—Default  
• When using sRTP Only—Displays when you check the SRTP Allowed check box  
For more information on security and trunks, see the Cisco Unified Communications Manager Security Guide. |
| 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. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:  
  
  - Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.  
  - Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  - On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  
  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 *Cisco Unified Communications Manager System Guide* for details of call behavior. If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified Communications Manager first tries to find an RSVP Agent 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 *Cisco Unified Communications Manager System Guide* for a complete discussion of network virtualization and trusted relay points. |
| PSTN Access                 | If you use the Cisco Intercompany Media Engine feature, check this check box to indicate that calls made through this trunk might reach the PSTN. Check this check box even if all calls through this trunk device do not reach the PSTN. For example, check this check box for tandem trunks or an H.323 gatekeeper routed trunk if calls might go to the PSTN.  
  
  When checked, this check box causes the system to create upload voice call records (VCRs) to validate calls made through this trunk device. By default, this check box remains checked. For more information on Cisco Intercompany Media Engine, see the *Cisco Intercompany Media Engine Installation and Configuration Guide*. |
**Field** | **Description**  
---|---  
Run On All Active Unified CM Nodes | To enable the trunk to run on every node, check this check box.  
Intercompany Media Engine (IME) |  
E.164 Transformation Profile | Check this check box if you want to use the Cisco Intercompany Media Engine and calls might reach the PSTN. For more information, see the Cisco Intercompany Media Engine Installation and Configuration Guide.  
From the drop-down list box, choose the appropriate E.164 transformation that you created on the Intercompany Media Services E.164 Transformation Configuration window (Advanced Features > Intercompany Media Services > E.164 Transformation).  
For more information on Cisco Intercompany Media Engine, see the Cisco Intercompany Media Engine Installation and Configuration Guide.  
Multilevel Precedence and Preemption (MLPP) Information |  
MLPP Domain | From the drop-down list, choose an MLPP domain to associate with this device. If you leave this field blank, this device inherits its MLPP domain from the value that is set for the device pool. If the device pool does not have an MLPP Domain setting, this device inherits its MLPP Domain from the value that is set for the MLPP Domain Identifier enterprise parameter.  
The default value for MLPP Domain specifies None.  
Call Routing Information |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Remote-Party-ID | Use this check box to allow or disallow the SIP trunk to send the Remote-Party-ID (RPID) header in outgoing SIP messages from Cisco Unified Communications Manager to the remote destination. If you check this box, the SIP trunk always sends the RPID header. If you do not check this box, the SIP trunk does not send the RPID header.  

**Note** Be aware that Calling Name Presentation, Connected Line ID, and Connected Name Presentation are not available when QSIG tunneling is enabled.  

**Outgoing SIP Trunk Calls**  
The configured values of the Calling Line ID Presentation and Calling Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted. **If** either option is set to Default, the corresponding information (Calling Line ID Presentation and/or Calling Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Cisco Unified Communications Manager. **If** either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window.  

**Incoming SIP Trunk Calls**  
The configured values of the Connected Line ID Presentation and Connected Name Presentation provide the basis for the construction of the Privacy field of the RPID header. Each of these two options can have the values of Default, Allowed, or Restricted.  

Be aware that the Connected Line ID Presentation and Connected Name Presentation options are relevant for 180/200 messages that the SIP trunk sends in response to INVITE messages that Cisco Unified Communications Manager receives.  

**If** either option is set to Default, the corresponding information (Connected Line ID Presentation and/or Connected Name Presentation) in the RPID header comes from the Call Control layer (which is based on call-by-call configuration) within Cisco Unified Communications Manager. **If** either option is set to Allowed or Restricted, the corresponding information in the RPID header comes from the SIP trunk configuration window.  

**Note** The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information.
### About trunk setup

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asserted Identity</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use this check box to allow or disallow the SIP trunk to send the Asserted-Type and SIP Privacy headers in SIP messages. If you check this check box, the SIP trunk always sends the Asserted-Type header; whether the SIP trunk sends the SIP Privacy header depends on the SIP Privacy configuration. If the check box is not selected, the SIP trunk does not include any Asserted-Type or SIP Privacy headers in its SIP messages. For more information, see the descriptions of Asserted-Type and SIP Privacy in this table.</td>
<td></td>
</tr>
<tr>
<td><strong>Outgoing SIP Trunk Calls—P Headers</strong></td>
<td>The decision of which Asserted Identity (either P-Asserted-Identity or P-Preferred-Identity) header gets sent depends on the configured value of the Asserted-Type option. A non-default value for Asserted-Type overrides values that come from Cisco Unified Communications Manager Call Control. If the Asserted-Type option is set to Default, the value of Screening Identification that the SIP trunk receives from Cisco Unified Communications Manager Call Control dictates the type of Asserted-Identity.</td>
</tr>
<tr>
<td><strong>Outgoing SIP Trunk Calls—SIP Privacy Header</strong></td>
<td>The SIP Privacy header gets used only when you check the Asserted Identity check box and when the SIP trunk sends either a PAI or PPI header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages). The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option. A non-default value for SIP Privacy overrides values that come from Cisco Unified Communications Manager Call Control. If the SIP Privacy option is set to Default, the Calling Line ID Presentation and Calling Name Presentation that the SIP trunk receives from Cisco Unified Communications Manager Call Control determines the SIP Privacy header.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>header. (Otherwise the SIP Privacy header neither gets sent nor processed in incoming SIP messages.)</td>
</tr>
<tr>
<td></td>
<td>The value of the SIP Privacy headers depends on the configured value of the SIP Privacy option.</td>
</tr>
<tr>
<td></td>
<td>A non-default value for SIP Privacy overrides values that come from Cisco Unified Communications Manager Call Control.</td>
</tr>
<tr>
<td></td>
<td>If the SIP Privacy option is set to Default, the Connected Line ID Presentation and Connected Name Presentation that the SIP trunk receives from Cisco Unified Communications Manager Call Control determine the SIP Privacy header.</td>
</tr>
<tr>
<td>Note</td>
<td>The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information.</td>
</tr>
<tr>
<td>Asserted-Type</td>
<td>From the drop-down list, choose one of the following values to specify the type of Asserted Identity header that SIP trunk messages should include:</td>
</tr>
<tr>
<td></td>
<td>• Default—This option represents the default value; Screening indication information that the SIP trunk receives from Cisco Unified Communications Manager Call Control determines the type of header that the SIP trunk sends.</td>
</tr>
<tr>
<td></td>
<td>• PAI—The Privacy-Asserted Identity (PAI) header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td></td>
<td>• PPI—The Privacy Preferred Identity (PPI) header gets sent in outgoing SIP trunk messages; this value overrides the Screening indication value that comes from Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Note</td>
<td>These headers get sent only if the Asserted Identity check box is checked.</td>
</tr>
</tbody>
</table>

**About trunk setup**
From the drop-down list, choose one of the following values to specify the type of SIP privacy header for SIP trunk messages to include:

- **Default**—This option represents the default value; Name/Number Presentation values that the SIP trunk receives from the Cisco Unified Communications Manager Call Control compose the SIP Privacy header. For example, if Name/Number presentation specifies Restricted, the SIP trunk sends the SIP Privacy header; however, if Name/Number presentation specifies Allowed, the SIP trunk does not send the Privacy header.

- **None**—The SIP trunk includes the Privacy:none header and implies Presentation allowed; this value overrides the Presentation information that comes from Cisco Unified Communications Manager.

- **ID**—The SIP trunk includes the Privacy:id header and implies Presentation restricted for both name and number; this value overrides the Presentation information that comes from Cisco Unified Communications Manager.

- **ID Critical**—The SIP trunk includes the Privacy:id;critical header and implies Presentation restricted for both name and number. The label critical implies that privacy services that are requested for this message are critical, and, if the network cannot provide these privacy services, this request should get rejected. This value overrides the Presentation information that comes from Cisco Unified Communications Manager.

**Note** These headers get sent only if the Asserted Identity check box is checked.

### Inbound Calls

**Significant Digits**

Significant digits represent the number of final digits that are retained on inbound calls. Use for the processing of incoming calls and to indicate the number of digits that are used to route calls that are coming in to the SIP device.

Choose the number of significant digits to collect, from 0 to 32, or choose All.

**Note** Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. The default value for Significant Digits specifies All.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Connected Line ID Presentation | Cisco Unified Communications Manager uses connected line ID presentation (COLP) as a supplementary service to provide the calling party with the connected party number. The SIP trunk level configuration takes precedence over the call-by-call configuration.  
   The default value for Connected Line ID Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send connected line information.  
   Choose Restricted if you do not want Cisco Unified Communications Manager to send connected line information.  
   If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed.  
   **Note**  
   Be aware that this service is not available when QSIG tunneling is enabled.  
   For more information about this field, see the *Cisco Unified Communications Manager System Guide*. |
| Connected Name Presentations  | Cisco Unified Communications Manager uses connected name ID presentation (CONP) as a supplementary service to provide the calling party with the connected party name. The SIP trunk level configuration takes precedence over the call-by-call configuration.  
   The default value for Connected Name Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send connected name information.  
   Choose Restricted if you do not want Cisco Unified Communications Manager to send connected name information.  
   **Note**  
   Be aware that this service is not available when QSIG tunneling is enabled. |
| Calling Search Space          | From the drop-down list box, choose the appropriate calling search space for the trunk. The calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number.  
   You can configure the number of items that display in this drop-down list box by using the Max List Box Items enterprise parameter. If more 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 Spaces window. Find and choose a calling search space name.  
   **Note**  
   To set the maximum list box items, choose **System > Enterprise Parameters** and choose CCMAdmin Parameters. The default value for Calling Search Space specifies None. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR Calling Search Space</td>
<td>Choose the appropriate calling search space for the device to use when performing automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. The default value for AAR Calling Search Space specifies None.</td>
</tr>
<tr>
<td>Prefix DN</td>
<td>Enter the prefix digits that are appended to the called party number on incoming calls. Cisco Unified Communications Manager adds prefix digits after first truncating the number in accordance with the Significant Digits setting. You can enter the international escape character +.</td>
</tr>
<tr>
<td>Redirecting Diversion Header</td>
<td>Check this check box to accept the Redirecting Number in the incoming INVITE message to the Cisco Unified Communications Manager. Uncheck the check box to exclude the Redirecting Number in the incoming INVITE message to the Cisco Unified Communications Manager. You use Redirecting Number for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should check the check box. The default value for Redirecting Number IE Deliver - Inbound specifies not checked.</td>
</tr>
</tbody>
</table>

**Incoming Calling Party Settings**

| Clear Prefix Setting          | To delete all prefixes for all calling party number types, click Clear Prefix Settings. |
| Default Prefix Setting        | To enter the default value for all prefix fields at the same time, click Default Prefix Settings. |
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 (#).
  
  If the word, Default, displays in the Prefix field, you cannot configure the Strip Digits field. 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, up to the number 24, 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**—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. 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.

  **Tip** For more information on configuring these settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

### Connected Party Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Device Pool Connected Party Transformation CSS</td>
<td>To use the Connected 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 Connected Party Transformation CSS that you configured for this device in the Trunk Configuration window.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Outbound Calls</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Use Device Pool Called Party Transformation CSS</strong></td>
<td>To use the Called 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 Called Party Transformation CSS that you configured for this device in the Trunk Configuration window.</td>
</tr>
<tr>
<td><strong>Use Device Pool Calling Party Transformation CSS</strong></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 Trunk Configuration window.</td>
</tr>
<tr>
<td><strong>Calling Party Selection</strong></td>
<td>Choose the directory number that is sent on an outbound call.</td>
</tr>
<tr>
<td><strong>Calling Line ID Presentation</strong></td>
<td>Cisco Unified Communications Manager uses calling line ID presentation (CLIP) as a supplementary service to provide the calling party number. The SIP trunk level configuration takes precedence over the call-by-call configuration. The default value for Calling Line ID Presentation specifies Default, which translates to Allowed. Choose Default if you want Cisco Unified Communications Manager to send calling number information. Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling number information.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>The following options specify which directory number is sent:</td>
</tr>
<tr>
<td></td>
<td>• Originator—Send the directory number of the calling device.</td>
</tr>
<tr>
<td></td>
<td>• First Redirect Number—Send the directory number of the redirecting device.</td>
</tr>
<tr>
<td></td>
<td>• Last Redirect Number—Send the directory number of the last device to redirect the call.</td>
</tr>
<tr>
<td></td>
<td>• First Redirect Number (External)—Send the external directory number of the redirecting device.</td>
</tr>
<tr>
<td></td>
<td>• Last Redirect Number (External)—Send the external directory number of the last device to redirect the call.</td>
</tr>
<tr>
<td></td>
<td>The default value for Calling Party Selection specifies Originator.</td>
</tr>
</tbody>
</table>
Cisco Unified Communications Manager uses calling name ID presentation (CNIP) as a supplementary service to provide the calling party name. The SIP trunk level configuration takes precedence over the call-by-call configuration.

Choose Allowed, which is the default, if you want Cisco Unified Communications Manager to send calling name information.

Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling name information.

The default value for Calling Name Presentation specifies Default.

**Note** Be aware that this service is not available when QSIG tunneling is enabled.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Calling Name Presentation | Cisco Unified Communications Manager uses calling name ID presentation (CNIP) as a supplementary service to provide the calling party name. The SIP trunk level configuration takes precedence over the call-by-call configuration.  
Choose Allowed, which is the default, if you want Cisco Unified Communications Manager to send calling name information. 
Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling name information. 
The default value for Calling Name Presentation specifies Default.  
**Note** Be aware that this service is not available when QSIG tunneling is enabled. |
| Caller ID DN       | Enter the pattern, from 0 to 24 digits, that you want to use to format the caller ID on outbound calls from the trunk.  
For example, in North America  
• 555XXXX = Variable Caller ID, where X represents an extension number. The Central Office (CO) appends the number with the area code if you do not specify it.  
• 5555000 = Fixed Caller ID. Use this form when you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.  
You can enter the international escape character +. |
<p>| Caller Name        | Enter a caller name to override the caller name that is received from the originating SIP Device. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling and Connected Party Info Format</td>
<td>This option allows you to configure whether Cisco Unified Communications Manager inserts a directory number, a directory URI, or a blended address that includes both the directory number and directory URI in the SIP identity headers for outgoing SIP messages. From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Deliver DN only in connected party—In outgoing SIP messages, Cisco Unified Communications Manager inserts the calling party's directory number in the SIP contact header information. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• Deliver URI only in connected party, if available—In outgoing SIP messages, Cisco Unified Communications Manager inserts the sending party's directory URI in the SIP contact header. If a directory URI is not available, Cisco Unified Communications Manager inserts the directory number instead.</td>
</tr>
<tr>
<td></td>
<td>• Deliver URI and DN in connected party, if available—In outgoing SIP messages, Cisco Unified Communications Manager inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Cisco Unified Communications Manager includes the directory number only.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You should set this field to Deliver URI only in connected party or Deliver URI and DN in connected party only if you are setting up URI dialing between Cisco Unified CM systems of release 9.0 or greater, or between a Cisco Unified CM system of release 9.0 or greater and a third party solution that supports URI dialing. Otherwise, you must set this field to Deliver DN only in connected party. For more information on URI dialing, see the URI dialing chapter in the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td>Redirecting Diversion Header Delivery - Outbound</td>
<td>Check this check box to include the Redirecting Number in the outgoing INVITE message from the Cisco Unified Communications Manager to indicate the original called party number and the redirecting reason of the call when the call is forwarded. Uncheck the check box to exclude the first Redirecting Number and the redirecting reason from the outgoing INVITE message. You use Redirecting Number for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number, you should check the check box. The default value for Redirecting Number IE Delivery - Outbound specifies check box does not get checked.</td>
</tr>
<tr>
<td>SIP Information</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destination Address</td>
<td>The Destination Address represents the remote SIP peer with which this trunk will communicate. The allowed values for this field specify a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is checked.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For configuring SIP trunks when you have multiple device pools in a cluster, you must configure a destination address that is a DNS SRV destination port. Enter the name of a DNS SRV port for the Destination Address and check the Destination Address is an SRV Destination Port check box.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Destination Address IPv6</td>
<td>The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. You can enter one of the following values in this field:</td>
</tr>
<tr>
<td></td>
<td>• A fully qualified domain name (FQDN)</td>
</tr>
<tr>
<td></td>
<td>• A DNS SRV record, but only if the Destination Address is an SRV field is checked.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field.</td>
</tr>
<tr>
<td>Destination Address is an SRV</td>
<td>This field specifies that the configured Destination Address is an SRV record.</td>
</tr>
<tr>
<td></td>
<td>The default value specifies unchecked.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Choose the destination port. Ensure that the value that you enter specifies any port from 1024 - 65535.</td>
</tr>
<tr>
<td>Note</td>
<td>You can now have the same port number that is specified for multiple trunks.</td>
</tr>
<tr>
<td></td>
<td>You need not enter a value if the destination address is an DNS SRV port. The default 5060 indicates the SIP port.</td>
</tr>
<tr>
<td></td>
<td>The default value for Destination Port specifies 5060.</td>
</tr>
<tr>
<td>MTP Preferred Originating Codec</td>
<td>Indicate the preferred outgoing codec:</td>
</tr>
<tr>
<td></td>
<td>• 711ulaw</td>
</tr>
<tr>
<td></td>
<td>• 711alaw</td>
</tr>
<tr>
<td></td>
<td>• G729/G729a</td>
</tr>
<tr>
<td></td>
<td>• G729b/G729ab</td>
</tr>
<tr>
<td>Note</td>
<td>To configure G.729 codecs for use with a SIP trunk, you must use a hardware MTP or transcoder that supports the G.729 codec. For more information, see the Cisco Unified Communications Manager System Guide.</td>
</tr>
<tr>
<td></td>
<td>This field gets used only when the MTP Termination Point Required check box is checked.</td>
</tr>
<tr>
<td>Presence Group</td>
<td>Configure this field with the Presence feature.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, choose a Presence group for the SIP trunk. The selected group specifies the destinations that the device/application/server that is connected to the SIP trunk can monitor.</td>
</tr>
<tr>
<td></td>
<td>The default value for Presence Group specifies Standard Presence group, which gets configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the drop-down list box.</td>
</tr>
<tr>
<td></td>
<td>Presence authorization works with presence groups to allow or block presence requests between groups. See the Cisco Unified Communications Manager Features and Services Guide for information about configuring permissions between groups.</td>
</tr>
<tr>
<td>Tip</td>
<td>You can apply a presence group to the SIP trunk or to the application that is connected to the SIP trunk. If a presence group is configured for both a SIP trunk and SIP trunk application, the presence group that is applied to the application overrides the presence group that is applied to the trunk.</td>
</tr>
</tbody>
</table>
Choose the security profile to apply to the SIP trunk.

You must apply a security profile to all SIP trunks that are configured in Cisco Unified Communications Manager Administration. Installing Cisco Unified Communications Manager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile.

To identify the settings that the profile contains, choose **System > Security Profile > SIP Trunk Security Profile**.

For information on how to configure security profiles, see the *Cisco Unified Communications Manager Security Guide*.

The default value for SIP Trunk Security Profile specifies Not Selected.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Trunk Security Profile</td>
<td>Choose the security profile to apply to the SIP trunk. You must apply a security profile to all SIP trunks that are configured in Cisco Unified Communications Manager Administration. Installing Cisco Unified Communications Manager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile. To identify the settings that the profile contains, choose <strong>System &gt; Security Profile &gt; SIP Trunk Security Profile</strong>. For information on how to configure security profiles, see the <em>Cisco Unified Communications Manager Security Guide</em>. The default value for SIP Trunk Security Profile specifies Not Selected.</td>
</tr>
<tr>
<td>Rerouting Calling Search Space</td>
<td>Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The rerouting calling search space gets used to determine where a SIP user (A) can refer another user (B) to a third party (C). After the refer is completed, B and C connect. In this case, the rerouting calling search space that is used is that of the initial SIP user (A). <strong>Note</strong> Calling Search Space also applies to 3xx redirection and INVITE with Replaces features. The default value for Rerouting Calling Search Space specifies None.</td>
</tr>
<tr>
<td>Out-of-Dialog Refer Calling Search Space</td>
<td>Calling search spaces determine the partitions that calling devices can search when they attempt to complete a call. The out-of-dialog calling search space gets used when a Cisco Unified Communications Manager refers a call (B) that is coming into SIP user (A) to a third party (C) when no involvement of SIP user (A) exists. In this case, the system uses the out-of-dialog calling search space of SIP user (A). The default value for Out-of-Dialog Refer Calling Search Space specifies None.</td>
</tr>
</tbody>
</table>
Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests from the device/server/application that connects to the SIP trunk. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the SIP trunk.

From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the SIP trunk. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box.

If you do not select a different calling search space for the SIP trunk from the drop-down list, the SUBSCRIBE calling search space defaults to None.

To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.

From the drop-down list box, choose the SIP profile that is to be used for this SIP trunk.

The default value for SIP Profile specifies None Selected.

Choose from the following options:

- No Preference (default)—Cisco Unified Communications Manager will pick the DTMF method to negotiate DTMF, so the call does not require an MTP. If Cisco Unified Communications Manager has no choice but to allocate an MTP (if the Media Termination Point Required check box is checked), SIP trunk will negotiate DTMF to RFC2833.
- RFC 2833—Choose this configuration if the preferred DTMF method to be used across the trunk is RFC2833. Cisco Unified Communications Manager makes every effort to negotiate RFC2833, regardless of MTP usage. Out of band provides the fallback method if the peer endpoint supports it.
- OOB and RFC 2833—Choose this configuration if both out of band and RFC2833 should be used for DTMF.

Note: If the peer endpoint supports both out of band and RFC2833, Cisco Unified Communications Manager will negotiate both out-of-band and RFC2833 DTMF methods. As a result, two DTMF events would get sent for the same DTMF keypress (one out of band and the other, RFC2833).
### About trunk setup

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normalization Script</td>
<td>From the drop-down list box, choose the script that you want to apply to this trunk.</td>
</tr>
<tr>
<td></td>
<td>To import another script, go to the SIP Normalization Script Configuration window (<a href="https://example.com">Device &gt; Device Settings &gt; SIP Normalization Script</a>), and import a new script file.</td>
</tr>
<tr>
<td>Parameter Name/Value</td>
<td>Optionally, enter parameter names and parameter values. Valid values include all characters except equals signs (=), semi-colons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Parameter Name Parameter Value</td>
</tr>
<tr>
<td></td>
<td>CCA-ID 1122344</td>
</tr>
<tr>
<td></td>
<td>pbx</td>
</tr>
<tr>
<td></td>
<td>location RTP</td>
</tr>
<tr>
<td></td>
<td>You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values.</td>
</tr>
<tr>
<td></td>
<td>To add another parameter line, click the + (plus) button. To delete a parameter line, click the - (minus) button.</td>
</tr>
<tr>
<td>Enable Trace</td>
<td>Check this check box to enable tracing within the script or uncheck this check box to disable tracing. When checked, the trace.output API provided to the Lua scripter produces SDI trace.</td>
</tr>
</tbody>
</table>
|                        | **Note**  
|                        | Cisco recommends that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.                                               |
| Geolocation Configuration | From the drop-down list box, choose a geolocation.                                                                                               |
| Geolocation            | You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.                                                                                  |
|                        | You can also choose a geolocation that has been configured with the **System > Geolocation Configuration** menu option.                                                                                 |
|                        | For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.          |
|                        | For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*. |

---

**Field:** Normalization Script  
**Description:** From the drop-down list box, choose the script that you want to apply to this trunk. To import another script, go to the SIP Normalization Script Configuration window ([Device > Device Settings > SIP Normalization Script](https://example.com)), and import a new script file.

**Field:** Parameter Name/Value  
**Description:** Optionally, enter parameter names and parameter values. Valid values include all characters except equals signs (=), semi-colons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value. Example:  
Parameter Name Parameter Value  
CCA-ID 1122344  
pbx  
location RTP  
You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values. To add another parameter line, click the + (plus) button. To delete a parameter line, click the - (minus) button.

**Field:** Enable Trace  
**Description:** Check this check box to enable tracing within the script or uncheck this check box to disable tracing. When checked, the trace.output API provided to the Lua scripter produces SDI trace.  
**Note**  
Cisco recommends that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.

**Field:** Geolocation Configuration  
**Description:** From the drop-down list box, choose a geolocation. You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation. You can also choose a geolocation that has been configured with the **System > Geolocation Configuration** menu option. For an explanation of geolocations, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*. For an overview and details of how logical partitioning uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*. 

---

*Cisco Unified Communications Manager Administration Guide, Release 9.1(1)*

644  
OL-27945-01
From the drop-down list box, choose a geolocation filter. If you leave the <None> setting, no geolocation filter gets applied for this device.

You can also choose a geolocation filter that has been configured with the System > Geolocation Filter menu option.

For an explanation of geolocation filters, including configuration details, see the Cisco Unified Communications Manager Features and Services Guide.

For an overview and details of how logical partitioning uses geolocation filters, see the Cisco Unified Communications Manager Features and Services Guide.

Send Geolocation Information
Check this check box to send geolocation information for this device.

For an overview and details of how logical partitioning uses geolocation information, see the Cisco Unified Communications Manager Features and Services Guide.

**Related Topics**
- Location setup, on page 107
- About calling search space setup, on page 247

**Find trunk**

Because you might have multiple trunks in your network, Cisco Unified Communications Manager lets you search for trunks on the basis of specified criteria. Follow these steps to search for a specific trunk in the Cisco Unified Communications Manager database.

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

**Procedure**

**Step 1**
Choose Device > Trunk.
The Find and List Trunks 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, on page 646.
To filter or search records
a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) 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.

---

**Related Topics**

Trunk setup, on page 591

---

## Set up trunk

Perform the following procedure to add a new trunk device or update an existing trunk device.

**Note**  
You can configure multiple trunk devices per Cisco Unified Communications Manager cluster.

**Before You Begin**

Configure SIP Trunk Security Profiles and SIP Profiles before you configure a SIP Trunk. For more information, see the related topics and the *Cisco Unified Communications Manager Security Guide*.

**Procedure**

**Step 1**  
Choose Device > Trunk.  
The Find and List Trunks window displays.

**Step 2**  
Perform one of the followings tasks:

a) To add a new trunk device, click the Add New button. The Trunk Configuration window displays. Continue with **Step 3**, on page 646.

b) To update trunk settings, locate the appropriate trunk. Click the name of the trunk that you want to update. Continue with **Step 7**, on page 647.

**Step 3**  
From the Trunk Type drop-down list, choose the type of trunk.

**Step 4**  
If applicable, from the Device Protocol drop-down list, choose the device protocol.

**Step 5**  
For SIP trunks, choose one of the following options from the Trunk Service Type drop-down list box:
a) None—Choose this option if the trunk will not be used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine.

b) Call Control Discovery—Choosing this option enables the trunk to support call control discovery. If you assign this trunk to the CCD advertising service in the Advertising Service window, the trunk handles inbound calls from remote call-control entities that use the SAF network. If you assign this trunk to the CCD requesting service in the Requesting Service window, the trunk handles outgoing calls to learned patterns. For more information on the call control discovery feature, see the Cisco Unified Communications Manager Features and Services Guide.

c) Extension Mobility Cross Cluster—Choosing this option enables the trunk to support the Extension Mobility Cross Cluster feature. For more information on the Extension Mobility Cross Cluster feature, see the Cisco Unified Communications Manager Features and Services Guide.

d) Cisco Intercompany Media Engine—Ensure that the Cisco IME server is installed and available before you configure this field.

Tip After you choose Call Control Discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine for the trunk service type and click Next, you cannot change the trunk to a different type.

Step 6 Click Next.

Step 7 On the Trunk Configuration window that displays, enter the appropriate settings for gatekeeper-controlled H.225 trunks, gatekeeper-controlled intercluster trunks, and non-gatekeeper-controlled intercluster trunks as described in Table 95: H.225 and intercluster trunks settings, on page 592. For SIP trunks, enter the appropriate settings as described in Table 96: SIP trunk settings, on page 619.

Step 8 To add the new trunk, click Save. The trunk gets added to the database.

If you are updating an existing trunk, click Apply Config to apply the new settings (this may also restart the device) and synchronize a trunk.

Note Resetting a trunk drops any calls in progress that are using that trunk. Restarting a gateway tries to preserve the calls in progress that are using that gateway, if possible. Other devices wait until calls complete before restarting or resetting. Resetting/restarting an H.323 or SIP device does not physically reset/restart the hardware; it only reinitializes the configuration that is loaded by Cisco Unified Communications Manager

Related Topics

- SIP trunk security profile setup, on page 147
- Trunk setup, on page 591
- H.225 and intercluster trunks settings, on page 592
- SIP trunk settings, on page 618
- Find trunk, on page 645
- Synchronize trunk, on page 649
- About SIP profile setup, on page 695

Delete trunk

Perform the following steps to delete a trunk.
Before You Begin

You cannot delete a trunk that is assigned to one or more route patterns. To find out which route patterns are using the trunk, in the Trunk Configuration window, choose Dependency Records from the Related Links drop-down list box and click Go. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message. If you try to delete a trunk that is in use, Cisco Unified Communications Manager displays a message. Before deleting a trunk that is currently in use, you must perform either or both of the following tasks:

- Assign a different trunk to any route patterns that are using the trunk that you want to delete.
- Delete the route patterns that are using the trunk that you want to delete.

Procedure

Step 1 Choose Device > Trunk. The Find and List Trunks window displays.

Step 2 To locate a specific trunk, enter search criteria and click Find. A list of trunks that match the search criteria displays.

Step 3 Perform one of the following actions:
   a) Check the check boxes next to the trunks that you want to delete and click Delete Selected.
   b) Delete all trunks in the window by clicking Select All and then clicking Delete Selected.
   c) From the list, choose the name of the trunk that you want to delete to display its current settings and click Delete. A confirmation dialog displays.

Step 4 To delete the trunk, click OK.

Related Topics

About route pattern setup, on page 189
Access dependency records, on page 874

Reset trunk

Perform the following procedure to reset the trunk.

Caution

Resetting devices can cause them to drop calls.

Procedure

Step 1 Choose Device > Trunk. The Find and List Trunks window displays.
Step 2 To locate a specific trunk, enter search criteria and click Find. A list of trunks that match the search criteria displays.

Step 3 From the list, click the name of the trunk that you want to reset. The Trunk Configuration window displays.

Step 4 After you change any settings for the Trunk Device, click Reset. The Device Reset dialog displays.

Step 5 Click one of the following choices:
   a) Restart—Restarts the trunk device without shutting it down first.
   b) Reset—Shuts down, then restarts, the internal trunk device. The Cisco Unified Communications Manager cluster unregisters (URQ) and then registers (RRQ) with the trunk if the trunk is gatekeeper controlled.
   c) Close—Closes the Reset Device dialog without performing any action.

   Note For SIP trunks, Restart and Reset behave the same way, so all active calls will disconnect when either choice is pressed. Trunks do not have to undergo a Restart or Reset when Packet Capture is enabled or disabled.

Related Topics
   Trunk setup, on page 591

Synchronize trunk

To synchronize a trunk with the most recent configuration changes, perform the following procedure, which applies 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 Device > Trunk. The Find and List Trunks window displays.

Step 2 Choose the search criteria to use.

Step 3 Click Find. The window displays a list of trunks that match the search criteria.

Step 4 Check the check boxes next to the trunks that you want to synchronize. To choose all trunks in the window, check the check box in the matching records title bar.

Step 5 Click Apply Config to Selected. The Apply Configuration Information dialog displays.

Step 6 Click OK.

Note Active calls may get disconnected during a restart.
Synchronize trunk
Device defaults setup

This chapter provides information to use device defaults to set the default characteristics of each type of device that registers with a Cisco Unified Communications Manager.

- About device defaults setup, page 651
- Device defaults settings, page 652
- Update device defaults, page 652

About device defaults setup

Use device defaults to set the default characteristics of each type of device that registers with a Cisco Unified Communications Manager. The device defaults for a device type apply to all auto-registered devices of that type within a Cisco Unified Communications Manager cluster. You can set the following device defaults for each device type to which they apply:

- Device load
- Device pool
- Phone button template

When a device auto-registers with a Cisco Unified Communications Manager, it acquires the device default settings for its device type. After a device registers, you can update its configuration individually to change the device settings.

Installing Cisco Unified Communications Manager automatically sets device defaults. You cannot create new device defaults or delete existing ones, but you can change the default settings.

Related Topics

- About device pool setup, on page 63
- Device defaults settings, on page 652
- Update device defaults, on page 652
- About phone button template setup, on page 671
Device defaults settings

The following table describes the settings for device defaults.

Table 97: Device defaults settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>This field displays the type of device for which device defaults can be set.</td>
</tr>
<tr>
<td>Protocol</td>
<td>This field displays the protocol that the corresponding device in the Device Type column uses.</td>
</tr>
<tr>
<td>Load Information</td>
<td>Enter the ID number of the firmware load that is used with a particular type of hardware device. If you install an upgrade or patch load, you must update the load information for each type of device that uses the new load.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Choose the device pool that is associated with each type of device. The device pool defines common characteristics for all devices in the pool.</td>
</tr>
<tr>
<td>Phone Template</td>
<td>Choose the phone button template that each type of Cisco Unified IP Phone uses. The template defines what keys on the phone perform that function.</td>
</tr>
</tbody>
</table>

Related Topics

Update device defaults, on page 652

Update device defaults

This section describes how to modify the device defaults in the Cisco Unified Communications Manager configuration database.

Before You Begin

Before updating the device defaults, perform any of the following tasks that apply to your system:

- Add new firmware files for the devices to the TFTP server.
- If you use device defaults to assign a firmware load that does not exist in the directory, those devices will fail to load the assigned firmware.
- Configure new device pools.
- If the device is a phone, configure new phone templates.
**Procedure**

**Step 1** Choose Device > Device Settings > Device Defaults.

**Step 2** Update the appropriate settings for the device that you want to change as described in Table 97: Device defaults settings, on page 652.

**Step 3** To save the changes in the Cisco Unified Communications Manager configuration database, click Save.

**Step 4** To reset all the devices of that type, click the Reset icon to the left of the device name and load the new defaults on all Cisco Unified Communications Managers in the cluster. If you choose not to reset all devices of that type, only new devices that are added after you change the device defaults receive the latest defaults.

**Related Topics**

- About device pool setup, on page 63
- About phone button template setup, on page 671
Device firmware load information

This chapter provides information to use device firmware load information to locate devices that are not using the default firmware load for their device type.

- Find devices with non-default firmware loads, page 655

Find devices with non-default firmware loads

The Firmware Load Information window in Cisco Unified Communications Manager Administration enables you to quickly locate devices that are not using the default firmware load for their device type.

Note

Each device can have an individually assigned firmware load that overrides the default.

Use the following procedure to locate devices that are not using the default firmware load.

Procedure

Step 1

Choose Device > Device Settings > Firmware Load Information. The page updates to display a list of device types that require firmware loads. For each device type, the Devices Not Using Default Load column links to configuration settings for any devices that use a non-default load.

Step 2

To view a list of devices of a particular device type that are using a non-default device load, click the entry for that device type in the Devices Not Using Default Load column. The window that opens lists the devices of a particular device type that are not running the default firmware load.
Find devices with non-default firmware loads
**Default device profile setup**

This chapter provides information about default device profile configuration.

- About default device profile setup, page 657
- Default device profile settings, page 657

### About default device profile setup

In Cisco Unified Communications Manager Administration, use the **Device > Device Settings > Default Device Profile** menu path to configure default device profiles.

Use the default device profile for whenever a user logs on to a phone model for which no user device profile exists. To create a default device profile for each phone model that supports Cisco Extension Mobility, use the Default Device Profile Configuration window. The maximum number of default device profiles cannot exceed the number of phone models that support Cisco Extension Mobility.

For example, a user logs on to a Cisco Unified IP Phone 7960, for which there is a user device profile. The user device profile for the user gets downloaded to the phone to which the user logged on. Later, the same user logs on to a Cisco Unified IP Phone 7940, for which he does not have a user device profile. In this case, the default device profile for the 7940 gets downloaded to the phone.

A default device profile comprises the set of attributes (services and/or features) that are associated with a particular device. The default device profile contains attributes such as device type, user locale, phone button template, expansion modules, softkey template, Join Across Lines and Single Button Barge feature settings, multilevel precedence and preemption (MLPP) information, and IP phone services.

### Default device profile settings

The following table describes the fields that are available in the Default Device Profile Configuration window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Device Profile Information</td>
<td></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 the default device profile configuration.</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
<td>To specify the audio source that plays when a user initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays. If you do not choose an audio source, Cisco Unified Communications Manager uses the audio source that is defined in the device pool or uses the system default if the device pool does not specify an audio source ID. <strong>Note</strong> You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Media Resources &gt; Music On Hold Audio Source.</td>
</tr>
<tr>
<td>User Locale</td>
<td>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. <strong>Note</strong> If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool. <strong>Note</strong> 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 Manager Locale Installer documentation.</td>
</tr>
<tr>
<td>Phone Button Template</td>
<td>Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.</td>
</tr>
<tr>
<td>Softkey Template</td>
<td>Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco Unified IP Phones. If the device pool contains the assigned softkey template, leave this field blank.</td>
</tr>
<tr>
<td>Privacy</td>
<td>From the drop-down list box, choose On for each phone on which you want privacy. For more configuration information, see the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
</tbody>
</table>
### Default device profile settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single Button Barge</strong></td>
<td>From the drop-down list box, choose from the following options:</td>
</tr>
<tr>
<td></td>
<td>- Off—This device does not allow users to use the Single Button Barge/cBarge feature.</td>
</tr>
<tr>
<td></td>
<td>- Barge—Choosing this option allows users to press the Single Button Barge shared-line button on the phone to barge into a call using Barge.</td>
</tr>
<tr>
<td></td>
<td>- cBarge—Choosing this option allows users to press the Single Button cBarge shared-line button on the phone to barge into a call using cBarge.</td>
</tr>
<tr>
<td></td>
<td>- Default—This device inherits the Single Button Barge/cBarge setting from the service parameter and device pool settings.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td><strong>Join Across Lines</strong></td>
<td>From the drop-down list box, choose from the following options:</td>
</tr>
<tr>
<td></td>
<td>- Off—This device does not allow users to use the Join Across Lines feature.</td>
</tr>
<tr>
<td></td>
<td>- On—This device allows users to join calls across multiple lines.</td>
</tr>
<tr>
<td></td>
<td>- Default—This device inherits the Join Across Lines setting from the service parameter and device pool settings.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the <em>Cisco Unified Communications Manager System Guide</em>.</td>
</tr>
<tr>
<td><strong>Always Use Prime Line</strong></td>
<td>From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received.</td>
</tr>
<tr>
<td></td>
<td>- On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls.</td>
</tr>
<tr>
<td></td>
<td>- Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Always Use Prime Line for Voice Message   | From the drop-down list box, choose one of the following options:  
  - **On**—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.  
  - **Off**—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.  
  - **Default**—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.                                                                                                                                                                    |
| Ignore Presentation Indicators (internal calls only) | Check the Ignore Presentation Indicators (internal calls only) check box to configure call display restrictions and ignore any presentation restriction that is received for internal calls.  
  **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 Cisco Unified Communications Manager Features and Services Guide.                                                                                      |
| Do Not Disturb                             | Check this check box to enable Do Not Disturb on the phone.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DND Option                                 | When you enable DND on the phone, this parameter allows you to specify how the DND features handle incoming calls:  
  - **Call Reject**—This option specifies that no incoming call information gets presented to the user, including no audio or visual 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.  
  - **Use Common Phone Profile Setting**—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device.  
  **Note** 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.                                                                                     |
### Field Description

**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 and for the DND Ringer Off option, incoming call information gets displayed. For the DND Call Reject option, no call alerts sound and no information gets sent to the device.

- **Flash Only**—For an incoming call, this option causes the phone to display a flash alert and for the DND Ringer Off option, incoming call information gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device.

### Multilevel Precedence and Preemption (MLPP) Information

**MLPP Domain**  
Choose MLPP domain that is associated with this device from the drop-down list box.

**MLPP Indication**  
If available, this setting specifies whether a device that is capable of playing precedence tones will use the capability when it places an MLPP precedence call.  
From the drop-down list box, choose a setting to assign to devices that use this default device profile from the following options:

- **Default**—This device inherits its MLPP indication setting from its device pool.

- **Off**—This device does not handle nor process indication of an MLPP precedence call.

- **On**—This device does handle and process 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 or Default (when default is Off) while MLPP Preemption is set to Forceful.

**Note**  
Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| MLPP Preemption              | If available, this 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 to assign to devices that use this default device profile from the following options:  
  - **Default**—This device inherits its MLPP preemption setting from its device pool.  
  - **Disabled**—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.  
  - **Forceful**—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. |

**Note**  
Do not configure a default device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

<table>
<thead>
<tr>
<th><strong>Logged Out (Default) Profile Information</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login User Id</strong></td>
<td>Enter a valid login user ID. If the user device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone automatically will log in to this login user ID.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Device Profile Defaults</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(listing of device profile defaults)</td>
<td>This pane displays a link to each default device profile that has been defined.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Default device profile setup, on page 657
- About default device profile setup, on page 657
Device profile setup

This chapter provides information to configure device profiles.

- About device profile setup, page 663
- Device profile setup tips, page 664
- Additional device profile setup features, page 664
- Device profile deletion, page 665
- Device profile settings, page 665

About device profile setup

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Device Profile menu path to configure device profiles.

A device profile comprises the set of attributes (services and/or features) that associate with a particular device. User device profiles include name, description, phone template, user locale, expansion modules, softkey templates, feature settings, MLPP information, directory numbers, subscribed services, and speed-dial information. You can assign the user device profile to a user, so, when the user logs in to a device, the user device profile that you have assigned to that user loads onto that device as a default login device profile. After a user device profile is loaded onto the phone, the phone picks up the attributes of that device profile.

You can also assign a user device profile to be the default logout device profile for a particular device. When a user logs out of a phone, for instance, the logout device profile loads onto the phone and gives that phone the attributes of the logout device profile. In the Cisco Unified CM Administration windows, you can create, modify, or delete the user device profile. If a user device profile is used as the logout device profile, you cannot delete the user device profile.

Cisco Unified Communications Manager also supports a device profile default. Use the device profile default for whenever a user logs on to a phone model for which no user device profile exists. To create a device profile default for each phone model that supports Cisco Extension Mobility, use the Device Profile Default Configuration window. The maximum number of device profile defaults cannot exceed the number of phone models that support Cisco Extension Mobility.

Related Topics
- Default device profile setup, on page 657
Device profile setup tips

Make sure that phone button template(s) are already configured before you configure the device profile. From the Association Info pane, you can configure directory numbers, speed dials, and intercom directory numbers for the device profile. For additional information about configuration settings, see the *Cisco Unified Communications Manager Features and Services Guide*.

If you click Modify Button Items, the Reorder Phone Button Configuration window opens. Use this window if you need to manage the phone button template button items.

**Note**

You must log in to a device for changes to a user device profile to take effect.

**Related Topics**

- Directory number setup, on page 263
- Cisco Unified IP Phone setup, on page 537
- Modify custom phone button template button items, on page 587
- About phone button template setup, on page 671

Additional device profile setup features

You can use the links in the Related Links drop-down list box at the top, right corner of the Device Profile Configuration window to perform additional configuration that is related to the device profile that you created. Use the following links to configure additional items:

- **Add a New Line Appearance**—To add a new line appearance to a device profile, select this link and click Go. The Directory Number Configuration window displays and allows you to configure a new DN that will associate to this device profile.

- **Add/Update Speed Dials**—To add or update the speed dial settings that are associated with a device profile, select this link and click Go. The Speed Dial and Abbreviated Dial Configuration window opens and allows you to configure the speed dial settings that will associate to this device profile.

- **Add/Update Busy Lamp Field Speed Dials**—To add or update the busy lamp field speed dial settings that are associated with a device profile, select this link and click Go. The Busy Lamp Field Speed Dial Configuration window opens and allows you to configure the busy lamp field speed dial settings that will associate to this device profile. See the *Cisco Unified Communications Manager Features and Services Guide* for configuration details of this window.

- **Add/Update Busy Lamp Field Directed Call Park**—To add or update the busy lamp field directed call park settings that are associated with a device profile, select this link and click Go. The Busy Lamp Field Directed Call Park Configuration window opens and allows you to configure the busy lamp field/directed call park settings that will associated to this device profile. See the *Cisco Unified Communications Manager Features and Services Guide* for configuration details of this window.

- **Add/Update Service URL Buttons**—To add or update the service URL buttons that are associated with a device profile, select this link and click Go. The Configure Service URL Buttons window opens and allows you to configure the service URL buttons that will associate to this device profile.
• Subscribe/Unsubscribe Services—To subscribe or unsubscribe IP phone services that are associated with a device profile, select this link and click Go. The Subscribed Cisco IP Phone Services window opens and allows you to subscribe or unsubscribe to Cisco IP Phone services that will associate to this device profile.

Related Topics

About directory number setup, on page 263
Set up speed-dial buttons or abbreviated dialing, on page 582
Set up IP phone services, on page 583
Service URL button setup, on page 585

Device profile deletion

You cannot delete a device profile if it is assigned to devices. To find out which devices are using the device profile, choose Dependency Records link from the Related Links drop-down list box in the Device Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a device profile that is in use, Cisco Unified Communications Manager displays message. Before deleting a device profile that is currently in use, you must perform either or both of the following tasks:

• Assign a different device profile to any devices that are using the device profile that you want to delete.
• Delete the devices that are using the device profile that you want to delete.

Note

If a user device profile is configured as a default logout device profile, you cannot delete it. If you want to delete a logout device profile, you must change it from a logout device profile and configure another device profile as the logout device profile for that phone. After the user device profile is no longer a logout device profile, you can delete it.

Related Topics

Access dependency records, on page 874

Device profile settings

The following table describes the available settings in the Device Profile Configuration window.

Table 99: Device profile settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Device Profile Information</td>
<td></td>
</tr>
<tr>
<td>Product Type</td>
<td>This field displays the product type to which this device profile applies.</td>
</tr>
<tr>
<td>Device Protocol</td>
<td>This field displays the device protocol to which this device profile applies.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Profile Name</td>
<td>Enter a unique name. This name can comprise up to 50 characters in length.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the device profile. For text, use anything that describes this</td>
</tr>
<tr>
<td></td>
<td>particular user device profile.</td>
</tr>
<tr>
<td>User Hold MOH Audio</td>
<td>To specify the audio source that plays when a user initiates a hold action, choose an audio</td>
</tr>
<tr>
<td>Source</td>
<td>source from the User Hold MOH Audio Source drop-down list box.</td>
</tr>
<tr>
<td></td>
<td>If you do not choose an audio source, Cisco Unified Communications Manager uses the audio</td>
</tr>
<tr>
<td></td>
<td>source that is defined in the device pool or the system default if the device pool does not</td>
</tr>
<tr>
<td></td>
<td>specify an audio source ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You define audio sources in the Music On Hold Audio Source Configuration window. For</td>
</tr>
<tr>
<td></td>
<td>access, choose <strong>Media Resources &gt; Music On Hold Audio Source</strong>.</td>
</tr>
<tr>
<td>User Locale</td>
<td>From the drop-down list box, choose the locale that is associated with the phone user</td>
</tr>
<tr>
<td></td>
<td>interface. The user locale identifies a set of detailed information, including language and font,</td>
</tr>
<tr>
<td></td>
<td>to support users.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager makes this field available only for phone models that</td>
</tr>
<tr>
<td></td>
<td>support localization.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If no user locale is specified, Cisco Unified Communications Manager uses the user</td>
</tr>
<tr>
<td></td>
<td>locale that is associated with the device pool.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the users require information to display (on the phone) in any language other than</td>
</tr>
<tr>
<td></td>
<td>English, verify that the locale installer is installed before configuring user locale. See the</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager Locale Installer documentation.</td>
</tr>
<tr>
<td>Phone Button Template</td>
<td>From the Phone Button Template drop-down list, choose a phone button template.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> If you want to configure BLF/SpeedDials for the profile for presence monitoring, choose</td>
</tr>
<tr>
<td></td>
<td>a phone button template that you configured for BLF/SpeedDials. After you save the configuration,</td>
</tr>
<tr>
<td></td>
<td>the Add a New BLF SD link displays in the Association Information pane. For more information on</td>
</tr>
<tr>
<td></td>
<td>BLF/SpeedDials, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Softkey Template</td>
<td>From the Softkey Template drop-down list box, choose the softkey template from the list that</td>
</tr>
<tr>
<td></td>
<td>displays.</td>
</tr>
<tr>
<td>Privacy</td>
<td>From the Privacy drop-down list box, choose On for each phone on which you want privacy.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Always Use Prime Line for Voice Message</td>
<td>From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.</td>
</tr>
<tr>
<td></td>
<td>• Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.</td>
</tr>
<tr>
<td></td>
<td>• Default—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.</td>
</tr>
<tr>
<td>Ignore Presentation Indicators (internal calls only)</td>
<td>To configure call display restrictions and ignore any presentation restriction that is received for internal calls, check the &quot;Ignore Presentation Indicators (internal calls only)&quot; check box.</td>
</tr>
<tr>
<td>Tip</td>
<td>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 <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>Check this check box to enable Do Not Disturb.</td>
</tr>
<tr>
<td>DND Option</td>
<td>When you enable DND on the phone, this parameter allows you to specify how the DND feature handles incoming calls:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Use Common Phone Profile Setting—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</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.                                                                                                                                                                                                                                                                                                                                                           |
| **Extension Mobility Cross Cluster CSS** | From the drop-down list box, choose an existing Calling Search Space (CSS) to use for this device profile for the Extension Mobility Cross Cluster feature. (To configure a new CSS or modify an existing CSS, choose **Call Routing > Class of Control > Calling Search Space** in Cisco Unified Communications Manager Administration.) Default value specifies None. The home administrator specifies this CSS, which gets used as the device CSS that gets assigned to the phone when the user logs in to this remote phone. For more information, see the Cisco Unified Communications Manager Features and Services Guide.                                                                                                                                                                                                 |
| **Expansion Module Information** | You can configure one or two expansion modules for this device profile by choosing phone templates from the expansion module drop-down lists in the expansion module fields.  
  **Note** You can view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate dialog box pops up and displays the phone buttons for that particular expansion module. Choose the appropriate expansion module or None.                                                                                                                                                                                                                       |
| **Module 1**          | You can configure one or two expansion modules for this device profile by choosing phone templates from the expansion module drop-down lists in the expansion module fields.  
  **Note** You can view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate dialog box pops up and displays the phone buttons for that particular expansion module. Choose the appropriate expansion module or None.                                                                                                                                                                                                                       |
| **Module 2**          | Choose the appropriate expansion module or None.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| **Multilevel Precedence and Preemption** | If this user device profile will be used for MLPP precedence calls, choose the MLPP Domain from the drop-down list box.  
  **Note** You define MLPP domains in the MLPP Domain Configuration window. For access, choose **System > MLPP Domain**.                                                                                                                                                                                                                                                                                                                                                              |
### Field | Description
--- | ---
MLPP Indication | If this user device profile will be used for MLPP precedence calls, assign an MLPP Indication setting to the device profile. This setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting to assign to this device profile from the following options:

1. **Default**—This device profile inherits its MLPP indication setting from the device pool of the associated device.
2. **Off**—This device does not handle nor process indication of an MLPP precedence call.
3. **On**—This device profile does handle and process indication of an MLPP precedence call.

**Note**  
Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

MLPP Preemption | If this user device profile will be used for MLPP precedence calls, assign an MLPP Preemption setting to the device profile. This setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call.

From the drop-down list box, choose a setting to assign to this device profile from the following options:

1. **Default**—This device profile inherits its MLPP preemption setting from the device pool of the associated device.
2. **Disabled**—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.
3. **Forceful**—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.

**Note**  
Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

Logged Out (Default) Profile Information

Login User Id | From the Login User ID drop-down list box, choose a valid login user ID.

**Note**  
If the device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone will automatically log in to this login user ID.

### Related Topics
- Device profile setup, on page 663
Phone button template setup

This chapter contains information about creating and using templates to assign a common button configuration to a large number of phones.

For example, if users in your company do not use the conference feature, you can create a template that reassigns this button to a different feature, such as speed dial. Make sure that all phones have at least one line that is assigned. Normally, use button 1 for this. You can assign additional lines to a phone, depending on the Cisco Unified IP Phone model. Phones also generally have several features, such as speed dial and call forward, that are assigned to the remaining buttons.

- About phone button template setup, page 671
- Phone button template deletion, page 672
- Phone button template settings, page 673
- Set up Cisco Unified IP Phone Expansion Module phone button template, page 673

About phone button template setup

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Phone Button Template menu path to configure phone button templates.

Cisco Unified Communications Manager includes default templates for each Cisco Unified IP Phone model. When you add phones, you can assign one of these templates to the phone or create a template of your own.

You can make changes to the custom, nonstandard templates that you created, and you can change the label of the custom phone button template. You cannot change the function of the buttons in the default templates.

You can update a custom, nonstandard phone button template to add or remove features, add or remove lines and speed dials, or assign features, lines, and speed dials to different buttons on the phone. You can change the button labels in the default phone button templates, but you cannot change the function of the buttons in the default templates. If you update a phone template, be sure to inform affected users of the changes.

The Programmable Line Key (PLK) feature expands the list of features that can be assigned to the line buttons to include features that are normally controlled by softkeys; for example, New Call, Call Back, End Call, and Forward All.

If you create a template for a Cisco Unified IP Phone, you can change the default template for that phone during autoregistration.
Phone button template configuration tips

If you are creating a custom, nonstandard phone button template, see the guidelines for creating new phone button templates. See the *Cisco Unified Communications Manager System Guide*.

Cisco Unified Communications Manager includes default templates for each Cisco Unified IP Phone model. When you add phones, you can assign one of these templates to the phone or create a template of your own.

If you create a template for a Cisco Unified IP Phone, you can change the default template for that phone during auto-registration.

---

**Note**

Renaming a template does not affect the phones that use that template. All Cisco Unified IP Phones that use this template continue to use this template after it is renamed. You can rename only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates.

---

**Note**

When you update a template, the change affects all phones that use the template. You can update only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates. After you update the template, click Reset to restart devices that use the template.

---

Phone button template deletion

You can delete phone templates that are not currently assigned to any phone in your system. You cannot delete a template that is assigned to one or more devices or device profiles or the default template for a model (which is specified in the Device Defaults Configuration window).

To find out which devices are using the phone button template, choose Dependency Records link from the Related Links drop-down list box in the Phone Button Template Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a phone button template that is in use, Cisco Unified Communications Manager displays a message. Before deleting a phone button template that is currently in use, you must perform either or both of the following tasks:

- Assign a different phone button template to any devices that are using the phone button template that you want to delete.
- Delete the devices that are using the phone button template that you want to delete.

---

**Note**

You can delete only phone button templates that display a check box in the left column. All other phone button templates serve as standard, read-only templates.

---

Related Topics

- Phone deletion preparation, on page 540
- About phone button template setup, on page 671
- Access dependency records, on page 874
Phone button template settings

The following table describes the phone button template settings.

Table 100: Phone button template settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Button Template Information</td>
<td>Enter a unique name that Cisco Unified Communications Manager uses to identify the template.</td>
</tr>
<tr>
<td>Button Template Name</td>
<td>Enter a unique name that Cisco Unified Communications Manager uses to identify the template.</td>
</tr>
<tr>
<td>Button Information</td>
<td>Choose the function of the phone button that you want to specify in the template. The programmable line key feature provides multiple features that can be assigned to line buttons; for example, MCID, DND, Call Park, Call Pickup, and many more.</td>
</tr>
<tr>
<td>Feature</td>
<td>Choose the function of the phone button that you want to specify in the template. The programmable line key feature provides multiple features that can be assigned to line buttons; for example, MCID, DND, Call Park, Call Pickup, and many more.</td>
</tr>
<tr>
<td>Note</td>
<td>You cannot change the function of buttons in default phone button templates.</td>
</tr>
<tr>
<td>Label</td>
<td>Enter a description of the button.</td>
</tr>
</tbody>
</table>

Related Topics

Phone button template setup, on page 671

Set up Cisco Unified IP Phone Expansion Module phone button template

You create a new phone button template for a Cisco Unified IP Phone Expansion Module by copying one of the Standard Cisco IP Phone phone button template, configuring the phone buttons, and saving the new phone button template.

Select a phone button template to copy by choosing the phone button template for the phone model that you are attaching the expansion module to. For example, if you are attaching an expansion module to a Cisco Unified IP Phone 9951, then you copy the Standard 9951 SIP phone button template. Use the following procedure to configure a Cisco Unified IP Phone Expansion Module.
Procedure

**Step 1** Find the phone button template by using the Find and List Phone Button Templates window (Device > Device Settings > Phone Button Template).

**Step 2** From the list of matching records, locate the phone button template that matches the phone model that you is being attached to the phone extension module and click the Copy icon.

**Step 3** For Button Template Name, enter a unique name for the phone button template (for example, Expansion Module 1).

**Step 4** Click Save.

**Step 5** Update the appropriate settings for Feature and Label as described in Table 100: Phone button template settings, on page 673 (the button template name that you just created will already display).

**Step 6** Click Save.
Softkey template setup

This chapter provides details about softkey template configuration. The administrator can copy, update, or delete nonstandard softkey templates by using softkey template configuration.

- About softkey template setup, page 675
- Find softkey template, page 675
- Create nonstandard softkey templates, page 676
- Add application softkeys to nonstandard softkey templates, page 677
- Set up softkey positions in nonstandard softkey templates, page 678
- Softkey template modification, page 679
- IP phone softkey template assignment, page 682

About softkey template setup

Softkey template configuration allows the administrator to manage softkeys that the Cisco Unified IP Phones (such as 7970) support. Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. Applications that support softkeys can have one or more standard softkey templates that are associated with them; for example, Cisco Unified Communications Manager has the Standard Feature and the Standard User softkey templates that are associated with it. You cannot modify standard softkey templates.

Find softkey template

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

**Procedure**

**Step 1** Choose Device > Device Settings > Softkey Template.
The Find and List Softkey Templates 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.
To filter or search records:

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.
d) From the third drop-down list box, select whether to search for standard, non-standard, or both types of softkey templates.

**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.

### Create nonstandard softkey templates

Cisco Unified Communications Manager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required.

**Procedure**

**Step 1** Choose Device > Device Settings > Softkey Template.
The Find and List Softkey Templates window displays.
Add application softkeys to nonstandard softkey templates

Cisco Unified Communications Manager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required. This procedure describes how to add application softkeys to a nonstandard softkey template that you created.

Procedure

Step 1  Find the softkey template.
Step 2  From the list of matching records, choose the softkey template to which you want to add application softkeys.

Note  You can modify only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

The Softkey Template Configuration window displays.

Step 3  To add additional application softkeys to the nonstandard softkey template, click the Add Application button. The Add Application window displays.
**Set up softkey positions in nonstandard softkey templates**

Cisco Unified Communications Manager includes standard softkey templates for call processing and applications. When creating custom, nonstandard softkey templates, copy the standard templates and make modifications as required. This procedure describes how to configure softkey positions for each call state in a nonstandard softkey template that you created.

**Procedure**

**Step 1** Find the softkey template by using the procedure in the [Find softkey template](#), on page 675.

**Step 2** From the list of matching records, choose the softkey template in which you want to configure softkey positions.

**Note** You can modify only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

The Softkey Template Configuration window displays.

**Step 3** To configure the positions of the softkeys on the Cisco Unified IP Phone LCD screen, choose Configure Softkey Layout from the Related Links drop-down list box; then, click Go.

The Softkey Layout Configuration window displays. The Select a call state to configure drop-down list box lists each Cisco Unified Communications Manager call state for an IP phone.

**Step 4** To configure the softkey positions for a call state, choose the call state from the Select a call state to configure drop-down list box.

The Softkey Layout Configuration window redisplay, and the Unselected Softkeys pane and Selected Softkeys pane display softkeys that are applicable to the call state that you chose.

**Tip** To create a relative place holder for a softkey, add the Undefined softkey. This allows the softkey that you added to occupy the same softkey position in all call states.
Step 5  To move softkeys from one list to the other, use the right and left arrows between the panes.
Step 6  To rearrange the positions of the Selected Softkeys, use the up and down arrows to the right of the Selected Softkeys pane.
Step 7  To save your softkey layout configuration, click Save.
Step 8  To return to the Softkey Template Configuration window, choose the Softkey Template Configuration link from the Related Links drop-down list box in the top, right-hand corner; then, click Go.
Step 9  To save your configuration, click Save.
Step 10 To make the updates of the softkey template take effect and synchronize the softkey template configuration with the phone, click Apply Config.

Related Topics
- Softkey template setup, on page 675
- Synchronize softkey template settings with devices, on page 681

Softkey template modification

You can make changes to custom, nonstandard softkey templates that you created.

Related Topics
- Rename softkey template, on page 679
- Delete softkey template, on page 680
- Update softkey template, on page 681
- Synchronize softkey template settings with devices, on page 681

Rename softkey template

Use this procedure to rename a nonstandard softkey template that you created.

Procedure

Step 1  Find the softkey template.
Step 2  From the list of matching records, choose the softkey template that you want to rename.
  **Note**  You can rename only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.
The Softkey Template Configuration page displays.
Step 3  In the Softkey Template Name field, enter the new name.
Step 4  Click Save.
The Softkey Template Configuration window redispays with the new softkey template name.
Delete softkey template

Use this procedure to delete a nonstandard softkey template that you created.

Before You Begin

You cannot delete a nonstandard softkey template that is currently assigned to a device or device pool. To find out which devices and device pools are using the nonstandard softkey template, choose Dependency Records from the Related Links drop-down list box in the Softkey Configuration window and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a nonstandard softkey template that is in use, Cisco Unified Communications Manager displays a message. Before deleting a nonstandard softkey template that is currently in use, you must perform either or both of the following tasks:

- Assign a different softkey template to any devices or device pools that are using the nonstandard softkey template that you want to delete.
- Delete the devices that are using the nonstandard softkey template that you want to delete.

Procedure

Step 1 Find the softkey template.

Step 2 From the list of matching records, choose the softkey template that you want to delete.

**Note** You can delete only softkey templates that display a check box in the left column. All other softkey templates represent standard, read-only templates.

The Softkey Template Configuration window displays.

Step 3 Click Delete.

**Note** You can delete multiple softkey templates from the Find and List Softkey Templates window by checking the check boxes next to the appropriate softkey templates and clicking Delete Selected.

You can delete all softkey templates in the window by clicking Select All and then clicking Delete Selected.

A message verifies that you want to delete the template.

Step 4 Click OK.

The Softkey Template Configuration window redisplays with the softkey template deleted.

Related Topics

- Phone deletion preparation, on page 540
- Find softkey template, on page 675
- IP phone softkey template assignment, on page 682
- Access dependency records, on page 874
**Update softkey template**

Use this procedure to update a nonstandard softkey template that you created. You can update the template name, description, application softkeys that are supported, and the softkey layout.

**Procedure**

1. **Step 1** Find the softkey template.
2. **Step 2** From the list of matching records, choose the softkey template that you want to update.
   - **Note** You can update only softkey templates that display a check box in the left column. All other softkey templates represent standard, read-only templates.
   - The Softkey Template Configuration window displays.
3. **Step 3** Update the settings that you want changed (such as adding an application softkey set or the softkey layout).
4. **Step 4** Click Save.
   - The Softkey Template Configuration window redisplays with the softkey template updated.
5. **Step 5** To apply the updated softkey template and synchronize the softkey template configuration with affected devices, click Apply Config.

**Related Topics**

- Softkey template setup, on page 675
- Find softkey template, on page 675
- Add application softkeys to nonstandard softkey templates, on page 677
- Set up softkey positions in nonstandard softkey templates, on page 678
- Synchronize softkey template settings with devices, on page 681

**Synchronize softkey template settings with devices**

To synchronize devices with a softkey template configuration that has undergone configuration changes, perform the following procedure, which applies 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 **Device > Device Settings > Softkey Template**.
   - The Find and List Softkey Templates window displays.
2. **Step 2** Choose the search criteria to use.
3. **Step 3** Click Find.
   - The window displays a list of softkey templates that match the search criteria.
Step 4  Click the softkey template to which you want to synchronize applicable devices. The Softkey Template 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.

IP phone softkey template assignment

You can assign softkey templates to IP phones when the phones are configured. You can assign standard and nonstandard softkey templates. Two ways to assign a softkey template to a phone exist:

- Assign the softkey template to a common device configuration and then assign the common device configuration to the phone in the Phone Configuration window.

- Assign the softkey template to the phone in the Softkey Template field in the Phone Configuration window.

Related Topics
   Set up Cisco Unified IP Phone, on page 577
   About common device setup, on page 713
IP phone services setup

This chapter provides information to configure IP phone services.

- About IP phone service setup, page 683
- IP phone service deletion, page 684
- IP phone service settings, page 685
- IP phone service parameter settings, page 688
- Set up IP phone service parameters, page 691
- IP phone service parameter deletion, page 692
- Add IP phone services to phone buttons, page 693

About IP phone service setup

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Phone Services menu path to configure IP phone services.

Using Cisco Unified Communications Manager Administration, you define and maintain the list of IP phone services that can display on supported Cisco Unified IP Phones models. IP phone services comprise XML applications or Cisco-signed Java MIDlets that enable the display of interactive content with text and graphics on some Cisco Unified IP Phones models.

Cisco Unified Communications Manager provides Cisco-provided default IP phone services, which install automatically with Cisco Unified Communications Manager. You can also create customized Cisco Unified IP Phone applications for your site.

After you configure the services, you can add services to the phones in the database, that is, if they are not classified as enterprise subscriptions, and you can assign the services to the Services, Directory, or Messages buttons/options, if the phone model supports these buttons/options. Users can log in to Cisco Unified CM User Options and subscribe to these services for their Cisco Unified IP Phones; that is, if these IP phone services are not classified as enterprise subscriptions.
IP phone services configuration tips

Caution
Do not put IP phone services on any Cisco Unified Communications Manager server at your site or any server that is associated with Cisco Unified Communications Manager, such as the TFTP server or publisher database server. This precaution eliminates the possibility that errors in an IP phone service application will have an impact on Cisco Unified Communications Manager performance or interrupt call-processing services.

If the service was modified after subscriptions existed, click Update Subscriptions to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed a phone service parameter, or changed the Parameter Name for a phone service parameter.

Note
If you change the service URL, remove an IP phone service parameter, or change the name of a phone service parameter for an IP phone service to which users are subscribed, be sure to click Update Subscriptions to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

Note
Cisco Unified Communications Manager allows you to create two or more IP phone services with identical names. Cisco recommends that you do not do so unless most or all phone users are advanced, or unless an administrator always configures the IP phone services. Be aware that if AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services.

Next steps after configuring an IP phone service
Configure the Services Provisioning setting, which displays in the Phone Configuration window, Common Phone Profile Configuration window, or Enterprise Parameter Configuration window.

IP phone service deletion

Tip
Cisco strongly recommends that you disable IP phone services, instead of deleting these services from Cisco Unified Communications Manager Administration. Disabling the IP phone service does not remove the service from the database, but it does ensure that the service does not display on the phone. Deleting the service removes the service from the database. You disable an IP phone service in the IP Phone Services Configuration window (Device > Device Settings > Phone Services) for the service that you want to disable.

When you delete an IP phone service, Cisco Unified Communications Manager removes all service information, user subscriptions, and user subscription data from the database. To find out which devices are using the IP phone service, from the IP phone service Configuration window, choose Dependency Records from the Related Records drop-down list box and click Go. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete an IP phone service that is in use, Cisco Unified Communications Manager displays a message. Before deleting an IP phone service that is currently in use, you must perform either or both of the following tasks:
• Assign a different IP phone service to any devices that are using the IP phone service that you want to delete.

• Delete the devices that are using the IP phone service that you want to delete.

**Related Topics**
- Phone deletion preparation, on page 540
- About IP phone service setup, on page 683
- Access dependency records, on page 874

## IP phone service settings

The following table describes the IP phone service settings that display in the IP Phone Services Configuration window in Cisco Unified Communications Manager Administration.

**Table 101: IP phone service settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Information</td>
<td></td>
</tr>
<tr>
<td>Service Name</td>
<td>Enter the name of the service. If the service is not marked as an enterprise subscription, the service name will display in areas where you can subscribe to a service; for example, under Cisco Unified CM User Options. Enter up to 128 characters for the service name. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file. <strong>Note</strong> Cisco Unified Communications Manager allows you to create two or more IP phone services with identical names. Cisco recommends that you do not do so unless most or all phone users are advanced, or unless an administrator always configures the IP phone services. Be aware that if AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services.</td>
</tr>
<tr>
<td>ASCII Service Name</td>
<td>Enter the name of the service to display if the phone cannot display Unicode.</td>
</tr>
<tr>
<td>Service Description</td>
<td>Enter a description of the content that the service provides. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), or single-quotes (').</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service URL</td>
<td>Enter the URL of the server where the IP phone services application is located. Make sure that this server remains independent of the servers in your Cisco Unified Communications Manager cluster. Do not specify a Cisco Unified Communications Manager server or any server that is associated with Cisco Unified Communications Manager (such as a TFTP server or directory database publisher server). For the services to be available, the phones in the Cisco Unified Communications Manager cluster must have network connectivity to the server. For Cisco-signed Java MIDlets, enter the location where the JAD file can be downloaded; for example, a web server or the backend application server to which the Java MIDlet communicates. For Cisco-provided default services, the service URL displays as Application:Cisco/&lt;name of service&gt; by default; for example, Application:Cisco/CorporateDirectory. If you modify the service URL for Cisco-provided default services, verify that you configured Both for the Service Provisioning setting, which displays in the Phone, Enterprise Parameter, and Common Phone Profile Configuration windows. For example, you use a custom corporate directory, so you change Application:Cisco/CorporateDirectory to the external service URL for your custom directory; in this case, change the Service Provisioning setting to Both.</td>
</tr>
<tr>
<td>Secure-Service URL</td>
<td>Enter the secure URL of the server where the Cisco Unified IP Phone services application is located. Make sure that this server remains independent of the servers in your Cisco Unified Communications Manager cluster. Do not specify a Cisco Unified Communications Manager server or any server that is associated with Cisco Unified Communications Manager (such as a TFTP server or publisher database server). For the services to be available, the phones in the Cisco Unified Communications Manager cluster must have network connectivity to the server. Note: If you do not provide a Secure-Service URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities.</td>
</tr>
<tr>
<td>Service Category</td>
<td>Select a service application type (XML or Java MIDlet). If you choose Java MIDlet, when the phone receives the updated configuration file, the phone retrieves the Cisco-signed MIDlet application (JAD and JAR) from the specified Service URL and installs the application.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Choose whether the service is provisioned to the Services, Directories, or Messages button/option on the phone; that is, if the phone has these buttons/options. To determine whether your phone these buttons/options, see the Cisco Unified IP Phone Administration Guide that supports your phone model.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Vendor</td>
<td>This field allows you to specify the vendor/manufacturer for the service. This field is optional for XML applications, but it is required for Cisco-signed Java MIDlets. For Cisco-signed Java MIDlets, the value that you enter in this field must exactly match the vendor that is defined in the MIDlet JAD file. This field displays as blank for Cisco-provided default services. You can enter up to 64 characters.</td>
</tr>
<tr>
<td>Service Version</td>
<td>Enter the version number for the application. For XML applications, this field is optional and is informational only. For Cisco-signed Java MIDlets, consider the following information: • If you enter a version, the service version must exactly match the version that is defined in the JAD file. If you enter a version, the phone attempts to upgrade or downgrade the MIDlet if the version is different than what is installed on the phone. • If the field is blank, the version gets retrieved from the Service URL. Leaving the field blank ensures that the phone attempts to download the JAD file every time that the phone reregisters to Cisco Unified Communications Manager as well as every time that the Cisco-signed Java MIDlet is launched; this ensures that the phone always runs the latest version of the Cisco-signed Java MIDlet without you having to manually update the Service Version field. This field displays as blank for Cisco-provided default services. You can enter numbers and periods in this field (up to 16 ASCII characters).</td>
</tr>
<tr>
<td>Enable</td>
<td>This check box allows you to enable or disable the service without removing the configuration from Cisco Unified Communications Manager Administration (and without removing the service from the database). Unchecking the check box removes the service from the phone configuration file and the phone.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>This check box allows you to automatically provision the service to all devices in the cluster that can support the service. If you check this check box, you (or an end user) cannot subscribe to the service. If this check box is unchecked, you must manually subscribe to the service for it to display on the phone (either in the Phone Configuration window, in BAT, or in the Cisco Unified CM User Options). Tip This setting displays only when you configure a service for the first time. After you save the service, the check box does not display in the window. To identify whether the service is provisioned to all devices in the cluster that can support the service, go to the Find and List IP Phone Services window and display the services. If true displays in the Enterprise Subscription column, you cannot manually subscribe to the service. If false displays, you can manually subscribe to the service; for example, an end user can subscribe to the service through the Cisco Unified CM User Options.</td>
</tr>
<tr>
<td>Subscription</td>
<td></td>
</tr>
</tbody>
</table>
This panel lists the service parameters that apply to this IP phone service. Use the following buttons to configure service parameters for this pane:

- **New Parameter**—Click this button to display the Configure Cisco Unified IP Phone Service Parameter window, where you configure a new service parameter for this IP phone service.
- **Edit Parameter**—Highlight a service parameter that displays in the Parameters pane, then click this button to display the Configure Cisco Unified IP Phone Service Parameter window, where you can edit the selected service parameter for this IP phone service.
- **Delete Parameter**—Highlight a service parameter that displays in the Parameters pane, then click this button to delete a service parameter for this IP phone service. A popup window asks you to confirm deletion.

**Related Topics**
- IP phone services setup, on page 683
- IP phone service parameter settings, on page 688

## IP phone service parameter settings

Add the IP phone service before you configure IP phone service parameters. See the documentation for the individual IP phone service for specific information about whether the service uses parameters, how those parameters should be configured, and whether you should provide optional parameter definitions.

**Tip**

If you remove an IP phone service parameter or change the parameter name of an IP phone service for an IP phone service to which users are subscribed, be sure to click Update Subscriptions to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

When you subscribe devices to the IP phone 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. Click Update Subscriptions only once and wait for this propagation to complete.

The following table describes the IP phone service parameter settings.

**Table 102: IP phone service parameter settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Service Parameter Information | This pane lists the service parameters that apply to this IP phone service. Use the following buttons to configure service parameters for this pane:  
- **New Parameter**—Click this button to display the Configure Cisco Unified IP Phone Service Parameter window, where you configure a new service parameter for this IP phone service.  
- **Edit Parameter**—Highlight a service parameter that displays in the Parameters pane, then click this button to display the Configure Cisco Unified IP Phone Service Parameter window, where you can edit the selected service parameter for this IP phone service.  
- **Delete Parameter**—Highlight a service parameter that displays in the Parameters pane, then click this button to delete a service parameter for this IP phone service. A popup window asks you to confirm deletion. |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Name</td>
<td>Enter the exact query string parameter to use when you build the subscription URL; for example, symbol.</td>
</tr>
<tr>
<td>Parameter Display Name</td>
<td>Enter a descriptive parameter name to display to the user in Cisco Unified CM User Options; for example, Ticker Symbol.</td>
</tr>
<tr>
<td>Default Value</td>
<td>Enter the default value for the parameter. This value displays to the user when a service is being subscribed to for the first time; for example, CSCO.</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>Enter a description of the parameter. The user can access the text that is entered here while the user is subscribing to the service. The parameter description should provide information or examples to help users input the correct value for the parameter. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Parameter is Required</td>
<td>If the user must enter data for this parameter before the subscription can be saved, check the Parameter is Required check box.</td>
</tr>
<tr>
<td>Parameter is a Password (mask contents)</td>
<td>You can mask entries in Cisco Unified CM User Options, so asterisks display rather than the actual user entry. You may want to do this for parameters such as passwords that you do not want others to be able to view. To mask parameter entry, check the Parameter is a Password (mask contents) check box in the Configure IP Phone Service Parameter window in Cisco Unified Communications Manager Administration.</td>
</tr>
</tbody>
</table>

### Cisco-provided default IP phone services

The following table displays the Cisco-provided default IP phone services that display if you specify the search parameter, IP Phone Service, and then click Find. Cisco Unified Communications Manager automatically provisions the Cisco-provided default services listed in the table.

To update these services, click the link in the Find and List IP Phone Service window. You can change the name of the service, where the default service displays on the phone, and the service URL. If you change the service URL for the default services, choose Both from the Service Provisioning drop-down list box, which displays in the Phone Configuration window, the Enterprise Parameter Configuration window, and the Common Phone Profile Configuration window.

---

**Tip**

Some Cisco Unified IP Phone models do not support IP phone services. To determine the support for your phone model, see the Cisco Unified IP Phone Administration Guide.
### Table 103: Cisco-provided default services

<table>
<thead>
<tr>
<th>Default Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Directory</td>
<td>This XML service allows the phone to display the corporate directory on the phone. By default, for phones with a Directory button/option, the corporate directory option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/CorporateDirectory. By default, the corporate directory automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service. If you update the corporate directory option because you want to configure this option to support a custom directory, for example, you update the Service URL to point to your custom directory, make sure that Both is chosen from the Service Provisioning drop-down list box, which displays in the Phone Configuration window, Enterprise Parameter Configuration window, or the Common Phone Profile Configuration window.</td>
</tr>
<tr>
<td>Intercom Calls</td>
<td>This XML service allows the phone to display the history records for intercom calls. By default, for phones with a Directory button/option, the intercom history option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/IntercomCalls. This service does not automatically display on all phones that support services in the cluster; therefore, you must manually subscribe to the service; for example, you can subscribe to the service in the Cisco Unified CM User Options.</td>
</tr>
<tr>
<td>Missed Calls</td>
<td>This XML service allows the phone to display missed calls on the phone. By default, for phones with a Directory button/option, the missed calls option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/MissedCalls. By default, the Missed Calls option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.</td>
</tr>
<tr>
<td>Personal Directory</td>
<td>This XML service allows a phone user to use Personal Directory. By default, for phones with a Directory button/option, the Personal Directory option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/PersonalDirectory. By default, the Personal Directory option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.</td>
</tr>
<tr>
<td>Placed Calls</td>
<td>This XML service allows the phone to display calls that the user has placed on the phone. By default, for phones with a Directory button/option, the placed calls option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/PlacedCalls. By default, the Placed Calls option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.</td>
</tr>
</tbody>
</table>
**Default Services**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Calls</td>
<td>This XML service allows the phone to display received calls on the phone. By default, for phones with a Directory button/option, the received calls option displays when a user presses the Directory button/option on the phone. By default, the service URL is Application:Cisco/ReceivedCalls. By default, the Received Calls option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.</td>
</tr>
<tr>
<td>Voicemail</td>
<td>This XML service allows users to retrieve voice messages on the phone. By default, for phones with a Messages button/option, the voice mail option displays when a user presses the Messages button/option on the phone. By default, the service URL is Application:Cisco/Voicemail. By default, the Voicemail option automatically displays on all phones that support services in the cluster, and you (or the end user) cannot subscribe to the service.</td>
</tr>
</tbody>
</table>

**Related Topics**

- IP phone services setup, on page 683

**Set up IP phone service parameters**

Use the following procedure to add and configure or update IP phone service parameters. Add the IP phone service before you configure parameters. See the documentation for the individual IP phone service for specific information about whether the service uses parameters, how those parameters should be configured, and whether you should provide optional parameter definitions.

**Procedure**

1. **Step 1** Find the IP phone service.
2. **Step 2** From the IP phone services list, choose the service to which you want to add parameters or update existing parameters. The IP Phone Services Configuration window displays.
3. **Step 3** Perform one of the followings tasks:
   a) To add a new IP phone service parameter, click the New button to the right of the Parameters list box. The Configure IP Phone Service Parameter window displays. Continue with Step 4, on page 691.
   b) To update an existing parameter, choose the name of the parameter that you want to update in the Parameters list box. Click Edit and continue with Step 4, on page 691.
4. **Step 4** Enter the appropriate settings as described in Table 102: IP phone service parameter settings, on page 688. To add the new parameter, click Save. To add additional parameters, if needed, click Add New in the Configure IP Phone Service Parameter window and repeat Step 3, on page 691 and Step 4, on page 691. To add the last parameter, click Save and Close.
   To apply the changes to the updated parameters, click Save, or to apply the changes and close the window, click Save and Close.
5. **Step 5** To apply the changes, update the IP Phone Services Configuration window.
a) If the service was modified after subscriptions existed, click Update Subscriptions to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed an IP phone service parameter, or changed the name for an IP phone service parameter.

**Note** If you remove an IP phone service parameter or change the parameter name of an IP phone service for an IP phone service to which users are subscribed, be sure to click Update Subscriptions to update all currently subscribed users with the changes. If you do not do so, users must resubscribe to the service to rebuild the URL correctly.

**Note** When you subscribe devices to the IP phone 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. Click Update Subscriptions only once and wait for this propagation to complete.

b) If the service is new and you do not need to rebuild user subscriptions, click Save.

### Related Topics

- IP phone services setup, on page 683

### IP phone service parameter deletion

Perform the following steps to delete an IP phone service parameter.

**Procedure**

**Step 1** Find the IP phone service by using Find and List IP Phone Services window (Device > Device Settings > Phone Services Phone Services).

**Step 2** From the IP phone services list, choose the IP phone service whose parameters you want to delete.

**Step 3** In the Parameters list box, choose the name of the parameter that you want to delete.

**Step 4** Click Delete Parameter.

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

**Step 5** To confirm the deletion, click OK.

**Step 6** To apply the changes, update the IP phone services configuration window:

a) If the service was modified after subscriptions existed, click Update Subscriptions to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed an IP phone service parameter, or changed the Parameter Name for an IP phone service parameter.

If you click Update Subscriptions more than once, an error occurs. 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.
b) If the service is new and you do not need to rebuild user subscriptions, click Save.

---

**Related Topics**

IP phone services setup, on page 683

---

### Add IP phone services to phone buttons

If you want to do so, you can assign the service to a phone button (a speed dial button) that is configured as a service URL.

By default, the IP phone service can display under the Directory, Message, or Services button/options on the phone, depending on your configuration in the IP Phone Services Configuration window, so you only need to add an IP phone service to a phone button if you want the service to display as a speed dial.

You can only perform this procedure for IP phone services that are not marked as enterprise subscriptions. Perform the following steps to add a service to a service URL button.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Add the service to Cisco Unified Communications Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Customize a phone button template by configuring a Service URL button.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add the customized phone button template to the phone.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Subscribe the service to the phone.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Add the service URL to a phone button.</td>
</tr>
</tbody>
</table>

---

**Related Topics**

Set up IP phone services, on page 583  
Service URL button setup, on page 585  
About phone button template setup, on page 671  
IP phone services setup, on page 683  
About IP phone service setup, on page 683
Add IP phone services to phone buttons
CHAPTER 78

SIP profile setup

This chapter provides information to configure and locate SIP profiles. A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that cannot be deleted or changed.

- About SIP profile setup, page 695
- SIP profile reset, page 695
- SIP profile deletion, page 695
- SIP profile settings, page 696
- Synchronize SIP profile settings with SIP devices, page 711

About SIP profile setup

A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. SIP profiles include information such as name, description, timing, retry, call pickup URI, and so on. The profiles contain some standard entries that cannot be deleted or changed.

SIP profile reset

For instructions on how to reset a SIP profile, see the descriptions of the Reset Selected and Reset buttons in the Cisco Unified Communications Manager System Guide.

Related Topics

Synchronize SIP profile settings with SIP devices, on page 711

SIP profile deletion

To find out which devices are using the SIP profile, choose Dependency Records link from the Related Links drop-down list box in the SIP 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 *Cisco Unified Communications Manager System Guide*.

**SIP profile settings**

The following table describes the available settings in the SIP Profile Configuration window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP Profile Information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name to identify the SIP profile; for example, SIP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>This field identifies the purpose of the SIP profile; for example, SIP for 7970. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>**Default MTP Telephony</td>
<td>This field specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. In most cases, the default value specifies the appropriate payload type. Be sure that you have a firm understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated. The default value specifies 101 with range from 96 to 127. The value of this parameter affects calls with the following conditions:</td>
</tr>
<tr>
<td><strong>Event Payload Type</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Namespace List</strong></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Early Offer for G.Clear Calls | The Early Offer for G.Clear Calls feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP). To enable or disable Early Offer for G.Clear Calls, choose one of the following options:  
  - Disabled  
  - CLEARMODE  
  - CCD  
  - G.nX64  
  - X-CCD |
| SDP Session-level Bandwidth Modifier for Early Offer and Re-invites | The Session Level Bandwidth Modifier specifies the maximum amount of bandwidth needed when all the media streams are used. There are three Session Level Bandwidth Modifiers: Transport Independent Application Specific (TIAS), Application Specific (AS), and Conference Total (CT). Select one of the following options to specify which Session Level Bandwidth Modifier to include in the SDP portion of SIP Early Offer or Reinvite requests.  
  - TIAS and AS  
  - TIAS only  
  - AS only  
  - CT only |
| Accept Audio Codec Preferences in Received Offer | Select On to enable Cisco Unified Communications Manager to honor the preference of audio codecs in received offer and preserve it while processing. Select Off to enable CUCM to ignore the preference of audio codecs in received offer and apply the locally configured Audio Codec Preference List. The default will select the service parameter configuration. |
Cisco Unified Communications Manager uses the Dial String Interpretation policy to determine if the SIP identity header is a directory number or directory URI.

Because directory numbers and directory URIs are saved in different database lookup tables, Cisco Unified Communications Manager examines the characters in the SIP identity header's user portion, which is the portion of the SIP address that is before the @ sign (for example, user@IP address or user@domain).

To configure the Dial String Interpretation, choose one of the following options from the drop-down list box:

- Always treat all dial strings as URI addresses—Cisco Unified Communications Manager treats the address of incoming calls as if they were URI addresses.

- Phone number consists of characters 0–9, A–D, *, and + (others treated as URI addresses)—Cisco Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI.

- Phone number consists of characters 0–9, *, and + (others treated as URI addresses)—Cisco Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI.

**Note** If the user=phone tag is present in the Request URI, Cisco Unified Communications Manager always treats the dial string as a number regardless of what option you choose for the Dial String Interpretation field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Dial String Interpretation | Cisco Unified Communications Manager uses the Dial String Interpretation policy to determine if the SIP identity header is a directory number or directory URI. Because directory numbers and directory URIs are saved in different database lookup tables, Cisco Unified Communications Manager examines the characters in the SIP identity header's user portion, which is the portion of the SIP address that is before the @ sign (for example, user@IP address or user@domain). To configure the Dial String Interpretation, choose one of the following options from the drop-down list box:  
  • Always treat all dial strings as URI addresses—Cisco Unified Communications Manager treats the address of incoming calls as if they were URI addresses.  
  • Phone number consists of characters 0–9, A–D, *, and + (others treated as URI addresses)—Cisco Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI.  
  • Phone number consists of characters 0–9, *, and + (others treated as URI addresses)—Cisco Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI.  
  
  **Note** If the user=phone tag is present in the Request URI, Cisco Unified Communications Manager always treats the dial string as a number regardless of what option you choose for the Dial String Interpretation field. |

| Redirect by Application | Checking this check box and configuring this SIP Profile on the SIP trunk allows the Cisco Unified Communications Manager administrator to:  
  • Apply a specific calling search space to redirected contacts that are received in the 3xx response.  
  • Apply digit analysis to the redirected contacts to make sure that the call get routed correctly.  
  • Prevent DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set.  
  • Allow other features to be invoked while the redirection is taking place.  
  Getting redirected to a restricted phone number (such as an international number) means that handling redirection at the stack level causes the call to be routed instead of being blocked. This behavior occurs if the Redirect by Application check box is unchecked. |
**Field**  
Disable Early Media on 180  

**Description**  
By default, Cisco Unified Communications Manager signals the calling phone to play local ringback if SDP is not received in the 180 or 183 response. If SDP is included in the 180 or 183 response, instead of playing ringback locally, Cisco Unified Communications Manager connects media, and the calling phone plays whatever the called device is sending (such as ringback or busy signal). If you do not receive ringback, the device to which you are connecting may be including SDP in the 180 response, but it is not sending any media before the 200OK response. In this case, check this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response.

**Note**  
Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device profile because it determines the behavior.

---

**Field**  
Outgoing T.38 INVITE Include Audio mline  

**Description**  
The parameter allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, you must also configure a SIP trunk with this SIP profile. For more information, see Chapter 68, Trunk "Configuration."

**Note**  
The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.

---

**Field**  
Enable ANAT  

**Description**  
This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. When you check both the Enable ANAT and the MTP 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 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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require SDP Inactive Exchange for Mid-Call</td>
<td>This feature designates how Cisco Unified Communications Manager handles mid-call updates to codecs or connection information such as IP address or port numbers. If the box is checked, during mid-call codec or connection updates Cisco Unified Communications Manager sends an INVITE a=inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls. <strong>Note</strong> For early offer enabled SIP trunks, this parameter will be overridden by the Send send-receive SDP in mid-call INVITE parameter. If the box is unchecked, Cisco Unified Communications Manager passes the mid-call SDP to the peer leg without sending a prior Inactive SDP to break the media exchange. This is the default behavior.</td>
</tr>
<tr>
<td>Media Change</td>
<td></td>
</tr>
<tr>
<td>Use Fully Qualified Domain Name in SIP</td>
<td>This feature enables Cisco Unified Communications Manager to relay an alphanumerichostname of a caller by passing it through to the called device or outbound trunk as a part of the SIP header information.</td>
</tr>
<tr>
<td>Requests</td>
<td>• If the box is unchecked, the IP address for Cisco Unified Communications Manager will be passed to the line device or outbound trunk instead of the user’s hostname. This is the default behavior.</td>
</tr>
<tr>
<td></td>
<td>• If the box is checked, Cisco Unified Communications Manager will relay an alphanumerichostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list. If the call is originating from a line device on the Cisco Unified Communications Manager cluster, and is being routed on a SIP trunk then the configured Organizational Top-Level Domain (e.g., cisco.com) will be used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the call is originating from a trunk on Cisco Unified Communications Manager and is being routed on a SIP trunk then:</td>
</tr>
<tr>
<td></td>
<td>◦ If the inbound call provides a host or domain in the caller’s information, the outbound SIP trunk messaging will preserve the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID.</td>
</tr>
<tr>
<td></td>
<td>◦ If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain will be used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID.</td>
</tr>
<tr>
<td>Assured Services SIP conformance</td>
<td>This checkbox should be checked for third-party AS-SIP endpoints as well as AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parameters used in Phone</td>
<td></td>
</tr>
<tr>
<td>Timer Invite Expires (seconds)</td>
<td>This field specifies the time, in seconds, after which a SIP INVITE expires. The Expires header uses this value. Valid values include any positive number; 180 specifies the default.</td>
</tr>
<tr>
<td>Timer Register Delta (seconds)</td>
<td>This field is intended to be used by SIP endpoints only. The endpoint receives this value via a tftp config file. The endpoint registers Timer Register Delta seconds before the registration period ends. The registration period gets determined by the value of the SIP Station KeepAlive Interval service parameter. Valid values for Timer Register Delta range from 32767 to 0. The default value is 5.</td>
</tr>
<tr>
<td>Timer Register Expires (seconds)</td>
<td>This field is intended to be used by SIP endpoints only. The SIP endpoint receives the value via a tftp config file. This field specifies the value that the phone that is running SIP sends in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value.</td>
</tr>
<tr>
<td></td>
<td>If the endpoint sends a shorter Expires value than the value of the SIP Station Keepalive Interval service parameter, Cisco Unified Communications Manager responds with a 423 &quot;Interval Too Brief&quot;.</td>
</tr>
<tr>
<td></td>
<td>If the endpoint sends an Expires value that is greater than the SIP Station Keepalive Interval service parameter value, Cisco Unified Communications Manager responds with a 200 OK that includes the Keepalive Interval value for Expires.</td>
</tr>
<tr>
<td>Note</td>
<td>For mobile phones that are running SIP, Cisco Unified Communications Manager uses the value in this field instead of the value that the SIP Station KeepAlive Interval service parameter specifies to determine the registration period.</td>
</tr>
<tr>
<td>Note</td>
<td>For TCP connections, the value for the Timer Register Expires field must be lower than the value for the SIP TCP Unused Connection service parameter.</td>
</tr>
<tr>
<td>Timer T1 (msec)</td>
<td>This field specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 500.</td>
</tr>
<tr>
<td>Timer T2 (msec)</td>
<td>This field specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 4000.</td>
</tr>
<tr>
<td>Retry INVITE</td>
<td>This field specifies the maximum number of times that an INVITE request gets retransmitted. Valid values include any positive number. Default specifies 6.</td>
</tr>
<tr>
<td>Retry Non-INVITE</td>
<td>This field specifies the maximum number of times that a SIP message other than an INVITE request gets retransmitted. Valid values include any positive number. Default specifies 10.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Start Media Port</td>
<td>This field designates the start real-time protocol (RTP) port for media. Media port ranges from 2048 to 65535. Default specifies 16384.</td>
</tr>
<tr>
<td>Stop Media Port</td>
<td>This field designates the stop real-time protocol (RTP) port for media. Media port ranges from 2048 to 65535. Default specifies 32766.</td>
</tr>
<tr>
<td>Call Pickup URI</td>
<td>This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the call pickup feature.</td>
</tr>
<tr>
<td>Call Pickup Group Other URI</td>
<td>This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the call pickup group other feature.</td>
</tr>
<tr>
<td>Call Pickup Group URI</td>
<td>This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the call pickup group feature.</td>
</tr>
<tr>
<td>Meet Me Service URI</td>
<td>This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the meet me conference feature.</td>
</tr>
<tr>
<td>User Info</td>
<td>This field configures the user= parameter in the REGISTER message. Valid values follow:</td>
</tr>
<tr>
<td></td>
<td>• none—No value gets inserted.</td>
</tr>
<tr>
<td></td>
<td>• phone—The value user=phone gets inserted in the To, From, and Contact Headers for REGISTER.</td>
</tr>
<tr>
<td></td>
<td>• ip—The value user=ip gets inserted in the To, From, and Contact Headers for REGISTER.</td>
</tr>
<tr>
<td>DTMF DB Level</td>
<td>This field specifies in-band DTMF digit tone level. Valid values follow:</td>
</tr>
<tr>
<td></td>
<td>• 1 to 6 dB below nominal</td>
</tr>
<tr>
<td></td>
<td>• 2 to 3 dB below nominal</td>
</tr>
<tr>
<td></td>
<td>• 3 nominal</td>
</tr>
<tr>
<td></td>
<td>• 4 to 3 dB above nominal</td>
</tr>
<tr>
<td></td>
<td>• 5 to 6 dB above nominal</td>
</tr>
<tr>
<td>Call Hold Ring Back</td>
<td>If you have a call on hold and are talking on another call, when you hang up the call, this parameter causes the phone to ring to let you know that you still have another party on hold. Valid values follow:</td>
</tr>
<tr>
<td></td>
<td>• Off permanently and cannot be turned on and off locally by using the user interface.</td>
</tr>
<tr>
<td></td>
<td>• On permanently and cannot be turned on and off locally by using the user interface.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Anonymous Call Block</td>
<td>This field configures anonymous call block. Valid values follow:</td>
</tr>
<tr>
<td></td>
<td>• Off—Disabled permanently and cannot be turned on and off locally by using the user interface.</td>
</tr>
<tr>
<td></td>
<td>• On—Enabled permanently and cannot be turned on and off locally by using the user interface.</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>This field configures caller ID blocking. When blocking is enabled, the phone blocks its own number or e-mail address from phones that have caller identification enabled. Valid values follow:</td>
</tr>
<tr>
<td></td>
<td>• Off—Disabled permanently and cannot be turned on and off locally by using the user interface.</td>
</tr>
<tr>
<td></td>
<td>• On—Enabled permanently and cannot be turned on and off locally by using the user interface.</td>
</tr>
<tr>
<td>Do Not Disturb Control</td>
<td>This field sets the Do Not Disturb (DND) feature. Valid values follow:</td>
</tr>
<tr>
<td></td>
<td>• User—The dndControl parameter for the phone should specify 0.</td>
</tr>
<tr>
<td></td>
<td>• Admin—The dndControl parameter for the phone should specify 2.</td>
</tr>
<tr>
<td>Telnet Level for 7940 and 7960</td>
<td>Cisco Unified IP Phones 7940 and 7960 do not support ssh for login access or HTTP that is used to collect logs; however, these phones support Telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values:</td>
</tr>
<tr>
<td></td>
<td>• Disabled (no access)</td>
</tr>
<tr>
<td></td>
<td>• Limited (some access but cannot run privileged commands)</td>
</tr>
<tr>
<td></td>
<td>• Enabled (full access)</td>
</tr>
<tr>
<td>Resource Priority Namespace</td>
<td>This field enables the admin to select one of the cluster’s defined Resource Priority Namespace network domains for assignment to a line via its SIP Profile.</td>
</tr>
<tr>
<td>Timer Keep Alive Expires</td>
<td>Cisco Unified Communications Manager requires a keepalive mechanism to support redundancy. This field specifies the interval between keepalive messages that are sent to the backup Cisco Unified Communications Manager to ensure that it is available in the event that a failover is required.</td>
</tr>
<tr>
<td>(seconds)</td>
<td></td>
</tr>
<tr>
<td>Timer Subscribe Expires</td>
<td>This field specifies the time, in seconds, after which a subscription expires. This value gets inserted into the Expires header field. Valid values include any positive number; however, 120 specifies the default value.</td>
</tr>
<tr>
<td>(seconds)</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Timer Subscribe Delta (seconds)</td>
<td>Use this parameter in conjunction with the Timer Subscribe Expires setting. The phone resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by Timer Subscribe Expires. Valid values range from 3 to 15. Default specifies 5.</td>
</tr>
<tr>
<td>Maximum Redirections</td>
<td>Use this configuration variable to determine the maximum number of times that the phone allows a call to be redirected before dropping the call. Default specifies 70 redirections.</td>
</tr>
<tr>
<td>Off Hook to First Digit Timer (microseconds)</td>
<td>This field specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set. The value ranges from 0 - 15,000 microseconds. Default specifies 15,000 microseconds.</td>
</tr>
<tr>
<td>Call Forward URI</td>
<td>This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the call forward feature.</td>
</tr>
<tr>
<td>Abbreviated Dial URI</td>
<td>This URI provides a unique address that the phone that is running SIP sends to Cisco Unified Communications Manager to invoke the abbreviated dial feature. Speed dials that are not associated with a line key (abbreviated dial indices) do not download to the phone. The phone uses the feature indication mechanism (INVITE with Call-Info header) to indicate when an abbreviated dial number has been entered. The request URI contains the abbreviated dial digits (for example, 14), and the Call-Info header indicates the abbreviated dial feature. Cisco Unified Communications Manager translates the abbreviated dial digits into the configured digit string and extend the call with that string. If no digit string has been configured for the abbreviated dial digits, a 404 Not Found response gets returned to the phone.</td>
</tr>
</tbody>
</table>
| Conference Join Enabled | This check box determines whether the Cisco Unified IP Phones 7940 or 7960, when the conference initiator that is using that phone hangs up, should attempt to join the remaining conference attendees. Check the check box if you want to join the remaining conference attendees; leave it unchecked if you do not want to join the remaining conference attendees.  
**Note** This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only. |
| RFC 2543 Hold | Check this check box to enable setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Cisco Unified Communications Manager. This allows backward compatibility with endpoints that do not support RFC3264. |
| Semi Attended Transfer | This check box determines whether the Cisco Unified IP Phones 7940 and 7960 caller can transfer the second leg of an attended transfer while the call is ringing. Check the check box if you want semi-attended transfer enabled; leave it unchecked if you want semi-attended transfer disabled.  
**Note** This check box applies to the Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only. |
### SIP Profile Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable VAD</td>
<td>Check this check box if you want voice activation detection (VAD) enabled; leave it unchecked if you want VAD disabled. When VAD is enabled, no media gets transmitted when voice is detected.</td>
</tr>
</tbody>
</table>
| Stutter Message Waiting    | Check this check box if you want stutter dial tone when the phone goes off hook and a message is waiting; leave unchecked if you do not want a stutter dial tone when a message is waiting.  
This setting supports Cisco Unified IP Phones 7960 and 7940 that run SIP. |
| MLPP User Authorization    | Check this box to enable MLPP User Authorization. MLPP User Authorization requires the phone to send in an MLPP username and password. |
| Call Stats                 | Check this check box if you want RTP statistics in BYE requests and responses enabled; leave unchecked if you want RTP statistics in BYE requests and responses disabled.  
If this check box is checked, the phone inserts the headers RTP-RxStat and RTP-TxStat as follows:  
\[
\begin{aligned}
\text{RTP-RxStat: } & \text{Dur}=a, \text{Pkt}=b, \text{Oct}=c, \text{LatePkt}=d, \text{LostPkt}=e, \text{AvgJit}=f \\
\text{RTP-TxStat: } & \text{Dur}=g, \text{Pkt}=h, \text{Oct}=i
\end{aligned}
\]
where:  
\begin{itemize}
  \item Dur—Total number of seconds since the beginning of reception or transmission.
  \item Pkt—Total number of RTP packets that are received or transmitted.
  \item Oct—Total number of RTP payload octets that are received or transmitted (not including RTP header).
  \item LatePkt—Total number of late RTP packets that are received.
  \item LostPkt—Total number of lost RTP packets that are received (not including the late RTP packets).
  \item AvgJit—Average jitter, which is an estimate of the statistical variance of the RTP packet interarrival time, measured in timestamp unit and calculated according to RFC 1889.
\end{itemize}
\begin{itemize}
  \item a, b, c, d, e, f, g, h, and i—Integers
\end{itemize} |
| Normalization Script       | From the drop-down list box, choose the script that you want to apply to this SIP profile.  
To import another script, go to the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script), and import a new script file. |
### Field Description

**Parameter Name/Parameter Value**
- Optionally, enter parameter names and parameter values. Valid values include all characters except equals signs (=), semi-colons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value.
- To add another parameter line, click the + (plus) button. To delete a parameter line, click the - (minus) button.
- **Note**: You must choose a script from the Normalization Script drop-down list box before you can enter parameter names and values.

**Enable Trace**
- Check this check box to enable tracing within the script or uncheck this check box to disable tracing. When checked, the trace.output API provided to the Lua scripter produces SDI trace
- **Note**: Cisco recommends that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.

### Incoming Requests FROM URI Settings

**Caller ID DN**
- Enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America:
  - 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it.
  - 55000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it.
- You can also enter the international escape character +.

**Caller Name**
- Enter a caller name to override the caller name that is received from the originating SIP Device.

### Trunk Specific Configuration
Cisco Unified Communications Manager only accepts calls from the SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Cisco Unified Communications Manager accepts the call, Cisco Unified Communications Manager uses the configuration for this setting to determine whether the call should get rerouted to another trunk.

From the drop-down list box, choose the method that Cisco Unified Communications Manager uses to identify the SIP trunk where the call gets rerouted:

- **Never**—If the SIP trunk matches the IP address of the originating device, choose this option, which equals the default setting. Cisco Unified Communications Manager, which identifies the trunk by using the source IP address of the incoming packet and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived.

- **Contact Info Header**—If the SIP trunk uses a SIP proxy, choose this option. Cisco Unified Communications Manager parses the contact header in the incoming request and uses the IP address or domain name and signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If no SIP trunk is identified, the call occurs on the trunk on which the call arrived.

- **Call-Info Header with purpose=x-cisco-origIP**—If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Cisco Unified Communications Manager parses the Call-Info header, looks for the parameter, purpose=x-cisco-origIP, and uses the IP address or domain name and the signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If the parameter does not exist in the header or no SIP trunk is identified, the call occurs on the SIP trunk on which the call arrived.

**Tip** This setting does not work for SIP trunks that are connected to a Cisco Unified Presence proxy server or SIP trunks that are connected to originating gateways in different Cisco Unified CM groups.

This field configures RSVP over SIP trunks. From the drop-down list box, choose the method that Cisco Unified Communications Manager uses to configure RSVP over SIP trunks:

- **Local RSVP**—In a local configuration, RSVP occurs within each cluster, between the end point and the local SIP trunk, but not on the WAN link between the clusters.

- **E2E**—In an end-to-end (E2E) configuration, RSVP occurs on the entire path between the end points, including within the local cluster and over the WAN.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fall back to local RSVP</td>
<td>Check this box if you want to allow failed end-to-end RSVP calls to fall back to local RSVP to establish the call. If this box is not checked, end-to-end RSVP calls that cannot establish an end-to-end connection fail.</td>
</tr>
<tr>
<td>SIP Rel1XX Options</td>
<td>This field configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) get sent reliably to the remote SIP endpoint. Valid values follow:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Disables SIP Rel1XX.</td>
</tr>
<tr>
<td></td>
<td>• Send PRACK if 1XX contains SDP—Acknowledges a 1XX message with PRACK, only if the 1XX message contains SDP.</td>
</tr>
<tr>
<td></td>
<td>• Send PRACK for all 1XX messages —Acknowledges all1XX messages with PRACK.</td>
</tr>
<tr>
<td></td>
<td>If you set the RSVP Over SIP field to E2E, you cannot choose Disabled.</td>
</tr>
<tr>
<td>Video Call Traffic Class</td>
<td>Video Call Traffic Class determines the type of video endpoint or trunk that the SIP Profile is associated with. From the drop-down list box, select one of the following three options</td>
</tr>
<tr>
<td></td>
<td>• Immersive—High-definition immersive video.</td>
</tr>
<tr>
<td></td>
<td>• Desktop—Standard desktop video.</td>
</tr>
<tr>
<td></td>
<td>• Mixed—A mix of immersive and desktop video.</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, &quot;Video Bandwidth&quot; and/or &quot;Immersive Bandwidth&quot;, depending on the type of call determined by the Video Call Traffic Class. Please refer to the Call Admission Control chapter of the Cisco Unified Communications Manager System Guide for more information.</td>
</tr>
<tr>
<td>Calling Line Identification Presentation</td>
<td>Select <strong>Strict From URI presentation Only</strong> to select the network provided identity.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Strict Identity Headers presentation Only</strong> to select the user provided identity.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deliver Conference Bridge Identifier</td>
<td>Check this check box for the SIP trunk to pass the b-number that identifies the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require that this field be enabled. Checking this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work. Enabling this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference.</td>
</tr>
<tr>
<td>Early Offer support for voice and video calls (insert MTP if needed)</td>
<td>Check this check box if you want to create a trunk that supports early offer. Early Offer configurations on SIP profile apply to SIP trunk calls. These configurations do not affect SIP line side calls. If this profile is shared between a trunk and a line, only the SIP trunk that uses the profile provides early offer. Because E2E RSVP provides an early offer by including an SDP in the initial INVITE, the early offer and E2E RSVP features are mutually exclusive on the SIP Profile Configuration window. When you choose E2E from the RSVP Over SIP drop-down list box, the Early Offer support for voice and video calls (insert MTP if needed) check box gets disabled. <strong>Note</strong> When checked, the Media Termination Required check box on the Trunk Configuration window overrides the early offer configuration on the associated SIP profile. The Cisco Unified Communications Manager sends the MTP IP address and port with a single codec in the SDP in the initial INVITE.</td>
</tr>
<tr>
<td>Send send-receive SDP in mid-call INVITE</td>
<td>Check this check box to prevent Cisco Unified Communications Manager from sending an INVITE a=inactive SDP message during call hold or media break during supplementary services. <strong>Note</strong> This check box applies only to early offer enabled SIP trunks and has no impact on SIP line calls. When you enable Send send-receive SDP in mid-call INVITE for an early offer SIP trunk in tandem mode, Cisco Unified Communications Manager inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a=inactive or sendonly or recvonly in audio media line. In tandem mode, Cisco Unified Communications Manager depends on the SIP devices to initiate reestablishment of media path by sending either a delayed INVITE or mid-call INVITE with send-recv SDP. When you enable both Send send-receive SDP in mid-call INVITE and Require SDP Inactive Exchange for Mid-Call Media Change on the same SIP Profile, the Send send-receive SDP in mid-call INVITE overrides the Require SDP Inactive Exchange for Mid-Call Media Change, so Cisco Unified Communications Manager does not send an INVITE with a=inactive SDP in mid-call codec updates. For SIP line side calls, the Require SDP Inactive Exchange for Mid-Call Media Change check box applies when enabled. <strong>Note</strong> To prevent the SDP mode from being set to inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter (System &gt; Service Parameters) to True.</td>
</tr>
</tbody>
</table>
### Field Description

| Allow Presentation Sharing using BFCP | If the box is checked, Cisco Unified Communications Manager is configured to allow supported SIP endpoints to use the Binary Floor Control Protocol to enable presentation sharing.  

The use of BFCP creates an additional media stream in addition to the existing audio and video streams. This additional stream is used to stream a presentation, such as a PowerPoint presentation from someone’s laptop, into a SIP videophone.  

If the box is unchecked, Cisco Unified Communications Manager rejects BFCP offers from devices associated with the SIP profile by setting the BFCP application line and associated media line ports to 0 in the answering SDP message. This is the default behavior.  

**Note** BFCP is only supported on SIP networks. BFCP must be enabled on all SIP trunks, lines, and endpoints for presentation sharing to work. BFCP is not supported if the SIP line or SIP trunk uses MTP, RSVP, TRP or Transcoder.  

For more information on BFCP, refer to the *Cisco Unified Communications Manager System Guide*. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow iX Application Media</td>
<td>Check this check box to enable support for iX media channel.</td>
</tr>
<tr>
<td>Allow Passthrough of Configured Line Device Caller Information</td>
<td>Check this box to allow passthrough of configured line device caller information from the SIP trunk.</td>
</tr>
<tr>
<td>Reject Anonymous Incoming Calls</td>
<td>Check this box to reject anonymous incoming calls.</td>
</tr>
<tr>
<td>Reject Anonymous Outgoing Calls</td>
<td>Check this box to reject anonymous outgoing calls.</td>
</tr>
</tbody>
</table>
| SIP OPTIONS Ping | Check this check box if you want to enable the SIP OPTIONS feature. SIP OPTIONS are requests to the configured destination address on the SIP trunk.  

If the remote SIP device fails to respond or sends back a SIP error response such as 503 Service Unavailable or 408 Timeout, Cisco Unified Communications Manager tries to reroute the calls by using other trunks or by using a different address.  

If this check box is not checked, the SIP trunk does not track the status of SIP trunk destinations.  

When this check box is checked, you can configure two request timers. |
This field configures the time duration between SIP OPTIONS requests when the remote peer is responding and the trunk is marked as In Service. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service.

The default value specifies 60 seconds. Valid values range from 5 to 600 seconds.

This field configures the time duration between SIP OPTIONS requests when the remote peer is not responding and the trunk is marked as Out of Service. The remote peer may be marked as Out of Service if it fails to respond to OPTIONS, if it sends 503 or 408 responses, or if the Transport Control Protocol (TCP) connection cannot be established. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service.

The default value specifies 120 seconds. Valid values range from 5 to 600 seconds.

This field specifies the maximum waiting time before retransmitting the OPTIONS request. Valid values range from 100 to 1000 milliseconds. The default value specifies 500 milliseconds.

This field specifies the number of times that Cisco Unified Communications Manager resends the OPTIONS request to the remote peer. After the configured retry attempts are used, the destination is considered to have failed. To obtain faster failure detection, keep the retry count low. Valid values range from 1 to 10. The default value specifies 6.

**Synchronize SIP profile settings with SIP devices**

To synchronize SIP devices with a SIP profile that has undergone configuration changes, perform the following procedure, which applies 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 **Device > Device Settings > SIP Profile**.

The Find and List SIP Profiles window displays.

**Step 2**  Choose the search criteria to use.

**Step 3**  Click Find.

The window displays a list of SIP Profiles that match the search criteria.
Step 4  Click the SIP profile to which you want to synchronize applicable SIP devices. The SIP Profile 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.
CHAPTER 79

Common device setup

This chapter provides information to configure common device configurations.

- About common device setup, page 713
- Common device setup deletion, page 713
- Common device settings, page 714
- Synchronize common device settings with devices, page 719

About common device setup

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Common Device Configuration menu path to configure common device configurations.

A common device configuration comprises user-specific service and feature attributes. Ensure that each device is associated with a common device configuration for user-oriented information.

Note

The Device Pool window now contains only location-related information. The Common Device Configuration window records all the user-oriented information.

Common device setup deletion

You cannot delete a common device configuration that a device uses. To find out which devices are using the common device configuration, click the Dependency Records link from the Common Device Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a common device configuration that is in use, Cisco Unified Communications Manager displays a message. Before deleting a common device configuration that is currently in use, you must perform either or both of the following tasks:

- Assign a different common device configuration to any devices that are using the common device configuration that you want to delete.
- Delete the devices that are using the common device configuration that you want to delete.
Common device settings

The following table describes the common device settings.

**Table 105: Common device settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Device Configuration Information</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify the common device configuration.</td>
</tr>
<tr>
<td>Softkey Template</td>
<td>From the drop-down list box, choose the softkey template for the common device configuration.</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
<td>Choose the audio source to use for MOH when a user initiates a hold action.</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
<td>Choose the audio source to use for music on hold (MOH) when the network initiates a hold action.</td>
</tr>
<tr>
<td>User Locale</td>
<td>From the drop-down list box, choose the locale for the common device configuration. The user locale identifies a set of detailed information to support users, including language and font. <strong>Note</strong> If the user does not choose a user locale, the locale that is specified in the Cisco Unified Communications Manager clusterwide parameters as Default User Locale applies.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Addressing Mode</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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 IPv4 address. If you choose this option, the SIP trunk uses an IPv6 address to connect to the peer device.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Signaling</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• IPv4—The dual-stack device prefers to establish a connection via an IPv4 address during a signaling event.</td>
</tr>
<tr>
<td></td>
<td>• IPv6—The dual-stack device prefers to establish a connection via an IPv6 address during a signaling event.</td>
</tr>
<tr>
<td></td>
<td>• Use System Default—The configuration for the enterprise parameter, IP Addressing Mode Preference for Signaling, applies.</td>
</tr>
</tbody>
</table>
### Field: Allow Auto-Configuration for Phones

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
</tr>
<tr>
<td><strong>On</strong> — 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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Tip</strong> — 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.</td>
</tr>
<tr>
<td><strong>Off</strong> — The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Default</strong> — To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option.</td>
</tr>
<tr>
<td>Although Cisco Unified Communications Manager does not use this configuration, the TFTP file that the phone obtains includes this information.</td>
</tr>
</tbody>
</table>

### Field: Use Trusted Relay Point

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the drop-down list box, choose one of the following options:</td>
</tr>
<tr>
<td><strong>On</strong> — To allow the IP Phones to send multicast echo request messages.</td>
</tr>
<tr>
<td><strong>Off</strong> — To disable sending multicast echo request messages.</td>
</tr>
<tr>
<td><strong>Default</strong> — To use the configuration for the Reply Multicast Echo Request enterprise parameter, choose this option.</td>
</tr>
</tbody>
</table>
Check this checkbox to enable the devices that associate with this common device configuration to use a trusted relay point.

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Cisco Unified Communications Manager inserts a TRP for an endpoint if the Use Trusted Relay Point check box is checked for the endpoint or for the common device configuration with which the endpoint associates. The endpoint device can comprise any device that terminates media, including SIP, H.323, MGCP, and SCCP devices, such as phones that are running SCCP, CTI devices, MoH servers, annunciators, and conference bridges.

If the Use Trusted Relay Point setting of a device specifies On or Off, the device setting overrides the Use Trusted Relay Point setting from the common device configuration with which the device associates.

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 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 Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Intercompany Media Engine (IME) for Outbound Calls</td>
<td>Check this check box to enable the devices that associate with this common device configuration to use a trusted relay point. A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified Communications Manager inserts a TRP for an endpoint if the Use Trusted Relay Point check box is checked for the endpoint or for the common device configuration with which the endpoint associates. The endpoint device can comprise any device that terminates media, including SIP, H.323, MGCP, and SCCP devices, such as phones that are running SCCP, CTI devices, MoH servers, annunciators, and conference bridges. If the Use Trusted Relay Point setting of a device specifies On or Off, the device setting overrides the Use Trusted Relay Point setting from the common device configuration with which the device associates. 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 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 Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.</td>
</tr>
</tbody>
</table>

Multilevel Precedence and Preemption Information
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Indication</td>
<td>This setting specifies whether devices that are capable of playing precedence tones will use the capability when the devices place an MLPP precedence call. From the drop-down list box, choose a setting to assign to the devices from the following options:</td>
</tr>
<tr>
<td></td>
<td>• Default—Devices inherit MLPP Indication settings from the MLPP Indication Status enterprise parameter.</td>
</tr>
<tr>
<td></td>
<td>• Off—Devices do not handle nor process indication of an MLPP precedence call.</td>
</tr>
<tr>
<td></td>
<td>• On—Devices do handle and process indication of an MLPP precedence call.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not configure the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Turning on MLPP Indication (at the enterprise parameter or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the device.</td>
</tr>
<tr>
<td>MLPP Preemption</td>
<td>This setting specifies whether devices that are capable of preempting calls in progress will use the capability when the devices place an MLPP precedence call. From the drop-down list box, choose a setting to assign to the devices from the following options:</td>
</tr>
<tr>
<td></td>
<td>• Default—Devices inherit MLPP Preemption settings from the MLPP Preemption Setting enterprise parameter.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Devices do not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.</td>
</tr>
<tr>
<td></td>
<td>• Forceful—Devices allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not configure the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.</td>
</tr>
<tr>
<td>MLPP Domain</td>
<td>From the drop-down list box, choose an MLPP domain that is associated with this common device configuration. If you leave the &lt;None&gt; setting, devices inherit MLPP domains from the value set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
</tbody>
</table>

**Related Topics**

Related Topics

- [Common device setup](#), on page 713
Synchronize common device settings with devices

To synchronize devices with a common device configuration that has undergone configuration changes, perform the following procedure, which applies 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 Device > Device Settings > Common Device Configuration. The Find and List Common Device Configurations window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find. The window displays a list of common device configurations that match the search criteria.

**Step 4** Click the common device configuration to which you want to synchronize applicable devices. The Common Device Configuration Information 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.

**Related Topics**

Common device setup, on page 713
Synchronize common device settings with devices
Common phone profile setup

This chapter provides information to configure and locate common phone profiles.

- About common phone profile setup, page 721
- Common phone profile deletion, page 721
- Common phone profile settings, page 722
- Synchronize common phone profile settings with devices, page 725

About common phone profile setup

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Common Phone Profile menu path to configure common phone profiles.

Common phone profiles provide data that Cisco TFTP requires. After you configure a common phone profile, use the Phone Configuration window to associate a phone that is running SCCP or SIP with a common phone profile.

Common phone profile deletion

To find out which devices are using the common phone profile, choose Dependency Records link from the Related Links drop-down list box in the Common Phone Profile Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

Note

You cannot delete the Standard Common Phone Profile.

Related Topics

Access dependency records, on page 874
Common phone profile settings

The following table describes the available settings in the Common Phone Profile Configuration window.

**Note** To view field descriptions and help for product-specific configuration items, click the ? question icon in the Product Specific Configuration area to display help in a popup window.

Select the "Override Common Settings" box for any setting in Product Specific Configuration area that you wish to update. If you do not check this box, the corresponding parameter setting does not take effect. Parameters that you set in the Product Specific Configuration area may also appear in the Device Configuration window for various devices and in the Enterprise Phone Configuration window. If you set these same parameters in these other windows too, the setting that takes precedence is determined in the following order: 1) Device Configuration window settings, 2) Common Phone Profile window settings, 3) Enterprise Phone Configuration window settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Phone Profile Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify the common phone profile; for example, CPP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Identify the purpose of the common phone profile; for example, common phone profile for the 7905 phone. The description can include up to 50 characters in any language, but it cannot include double-quotes (&quot;), percentage sign (%), ampersand (&amp;), back-slash (), or angle brackets (&lt;&gt;).</td>
</tr>
<tr>
<td>Local Phone Unlock Password</td>
<td>Enter the password that is used to unlock a local phone. Valid values comprise 1 to 15 characters.</td>
</tr>
<tr>
<td>DND Option</td>
<td>When you enable Do Not Disturb (DND) on the phone, this parameter allows you to specify how the DND features handle incoming calls:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so the user can accept the call.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**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:
- **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 beep.
- **Flash Only**—For an incoming call, this option causes the phone to display a flash alert.

**Feature Control Policy** | From the drop-down list box, you can choose a feature control policy that has already been configured in the Feature Control Policy configuration window (Device > Device Settings > Feature Control Policy).

**Enable End User Access to Phone Background Image Setting** | Check this check box to enable end users to change the background image on phones that use this common phone profile.

**Secure Shell Information** | Enter a user ID for the secure shell user. Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance.
See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified Communications Manager does not send SSH credentials to the phone in the clear.

**Secure Shell User** | Enter the password for a secure shell user. Contact TAC for further assistance.
See the Cisco Unified Communications Manager Security Guide for this release for information about how to configure encrypted phone configuration files to ensure that Cisco Unified Communications Manager does not send SSH passwords to the phone in the clear.

**Phone Personalization Information** |
### Phone Personalization

The Phone Personalization setting allows you to enable a Cisco Unified IP Phone, so it works with Phone Designer, a Cisco Unified Communications widget that allows a phone user to customize the wallpaper and ring tones on the phone. From the Phone Personalization drop-down list box, choose one of the following options:

- **Disabled**—The user cannot customize the Cisco Unified IP Phone by using Phone Designer.
- **Enabled**—The user can use Phone Designer to customize the phone.
- **Default**—The phone uses the configuration from the Phone Personalization enterprise parameter if you choose Default in both the Phone Configuration and Common Phone Profile Configuration windows. If you choose Default in the Common Phone Profile Configuration window but not in the Phone Configuration window, the phone uses the configuration that you specify in the Phone Configuration window.

You must install and configure Phone Designer, so the phone user can customize the phone. Before you install and configure Phone Designer, identify which Cisco Unified IP Phone models work with Phone Designer, as described in the Phone Designer documentation. For more information on Phone Designer, see the Phone Designer documentation.

### Always Use Prime Line

From the drop-down list box, choose one of the following options:

- **Off**—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received.
- **On**—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls.
- **Default**—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.

### Always Use Prime Line for Voice Message

From the drop-down list box, choose one of the following options:

- **On**—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.
- **Off**—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.
- **Default**—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.
From the drop-down list box, choose how the phone will support the services:

• **Internal**—The phone uses the phone configuration file to support the service. Choose this option or Both for Cisco-provided default services where the Service URL has not been updated; that is, the service URL indicates Application:Cisco/<name of service>; for example, Application:Cisco/CorporateDirectory.

Choose Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file.

• **External URL**—Choosing External URL indicates that the phone ignores the services in the phone configuration file and retrieves the services from a Service URL.

If you configured a custom Service URL for a service, you must choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the phone.

• **Both**—Choosing Both indicates that the phone support both the services that are defined in the configuration file and external applications that are retrieved from custom service URLs.

If you have phones in your network that can obtain the service information from the phone configuration file and phones in your network that can only use custom service URLs for obtaining the information, choose Both.

### Related Topics

- Common phone profile setup, on page 721

---

## Synchronize common phone profile settings with devices

To synchronize devices with a common phone profile that has undergone configuration changes, perform the following procedure, which applies 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 Device > Device Settings > Common Phone Profile. The Find and List Common Phone Profiles window displays.

**Step 2** Choose the search criteria to use.

**Step 3** Click Find. The window displays a list of common phone profiles that match the search criteria.

**Step 4** Click the common phone profile to which you want to synchronize applicable devices. The Common Phone Profile 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.

**Related Topics**

Common phone profile setup, on page 721
Feature Control Policy setup

This chapter provides information to find and add Feature Control Policies. When you disable a feature, the softkeys for the disabled feature do not appear in any call state.

- About Feature Control Policy setup, page 727
- Feature Control Policy deletion, page 728
- Feature Control Policy settings, page 729
- Feature Control Policy default values, page 729

About Feature Control Policy setup

To generate a list of supported features for all phones on your Cisco Unified Communications Manager, including the Feature Control Policy, you can generate a Unified CM Phone Feature List report on Cisco Unified Reporting.

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Feature Control Policy menu path to configure feature control policies.

Feature Control Policies allows you to enable or disable a particular feature and thereby control the appearance of certain features and softkeys that display on the phone. You can configure multiple policies on Cisco Unified Communications Manager Administration. After you configure a Feature Control Policy, you must associate that policy to an individual phone, a group of phones, or to all phones in the system.

Note

You can customize the appearance of softkeys on other Cisco Unified IP Phones by using softkey templates.

Feature control policies configuration tips

When you configure a feature control policy, specify the phone to which you want the feature control policy to apply. You can set feature control policies for all phones in your system, for a group of phones, or for an individual phone. You can also have multiple feature control policies.

- To specify a policy for all phones on the system, choose System > Enterprise Parameters and select the feature control policy that you want from the Feature Control Policy drop-down box in the Enterprise Parameters window.
• To specify a policy to a group of phones, choose Device > Phone > Common Phone Profile to create a new phone profile or to update an existing phone profile, select the feature control policy that you want in the Feature Control Policy drop-down box, and then select the common phone profile when you configure your phone.

• To specify a policy on an individual phone, choose Device > Phone, and select the feature control policy that you want from the Feature Control Policy drop-down box in the Phone Configuration window.

---

**Note**

When feature control polices are configured in different windows, Cisco Unified Communications Manager uses the following order of precedence (Device Configuration has the highest precedence):

1. Device Configuration window settings
2. Common Phone Profile window settings
3. Enterprise Parameter Configuration window settings

---

**Related Topics**

- Update enterprise parameters, on page 128
- Phone setup, on page 539
- About common phone profile setup, on page 721
- Feature Control Policy default values, on page 729

---

**Feature Control Policy deletion**

You can delete a feature control policy that is not currently assigned to any phone in your system. You cannot delete a policy that is assigned to one or more phones.

To find out which phones are using the feature control policy, choose the Dependency Records link from the Related Links drop-down list box in the Feature Control Policy Configuration window and click Go. If dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a feature control policy that is in use, Cisco Unified Communications Manager displays a message. Before deleting a feature control policy that is currently in use, you must perform either or both of the following tasks:

• Assign a different feature control policy to the phones that are using the feature control policy that you want to delete.

• Delete the phones that are using the feature control policy that you want to delete.

**Related Topics**

- Phone deletion preparation, on page 540
- About Feature Control Policy setup, on page 727
- Access dependency records, on page 874
Feature Control Policy settings

The following table describes the Feature Control Policy settings.

Table 107: Feature Control Policy settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Control Policy Info</td>
<td>Enter a name in the Feature Control Policy 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 feature control policy name is unique to the system.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a description in the Description field. The description can comprise up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_).</td>
</tr>
<tr>
<td>Feature Control Section</td>
<td></td>
</tr>
<tr>
<td>Feature Control</td>
<td>For each feature listed, choose whether you want to override the system default and enable or disable the setting: • If the feature is enabled by default and you want to disable the setting, check the check box under Override Default and uncheck the check box under Enable Setting. • If the feature is disabled by default and you want to enable the setting, check the check box under Override Default and check the check box under Enable Setting.</td>
</tr>
</tbody>
</table>

Feature Control Policy default values

The following table lists the features, default value, and associated softkeys for feature control policies.

Table 108: Feature Control Policy default values

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Value</th>
<th>Softkeys Displayed on the Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barge</td>
<td>Enabled</td>
<td>Barge</td>
</tr>
<tr>
<td>Call Back</td>
<td>Enabled</td>
<td>Call Back</td>
</tr>
<tr>
<td>Call Pick Up</td>
<td>Disabled</td>
<td>Call Pick Up</td>
</tr>
<tr>
<td>Conference List</td>
<td>Enabled</td>
<td>Show Detail</td>
</tr>
</tbody>
</table>
### Feature Control Policy default values

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Value</th>
<th>Softkeys Displayed on the Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Divert (Alerting)</td>
<td>Disabled</td>
<td>Divert</td>
</tr>
<tr>
<td>Divert (Connected)</td>
<td>Disabled</td>
<td>Divert</td>
</tr>
<tr>
<td>Forward All</td>
<td>Enabled</td>
<td>Forward All</td>
</tr>
<tr>
<td>Group Call Pick Up</td>
<td>Disabled</td>
<td>Group Call Pick Up</td>
</tr>
<tr>
<td>Meet Me</td>
<td>Disabled</td>
<td>Meet Me</td>
</tr>
<tr>
<td>Mobility</td>
<td>Disabled</td>
<td>Mobility</td>
</tr>
<tr>
<td>Other Call Pick Up</td>
<td>Disabled</td>
<td>Other Call Pick Up</td>
</tr>
<tr>
<td>Park</td>
<td>Disabled</td>
<td>Park and Resume</td>
</tr>
<tr>
<td>Redial</td>
<td>Enabled</td>
<td>Redial</td>
</tr>
<tr>
<td>Report Caller</td>
<td>Disabled</td>
<td>Report Caller</td>
</tr>
<tr>
<td>Report Quality</td>
<td>Disabled</td>
<td>Report Quality</td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Enabled</td>
<td>Speed Dial</td>
</tr>
</tbody>
</table>

**Related Topics**

Feature Control Policy setup, on page 727
CHAPTER 82

Recording Profile setup

This chapter provides information to configure recording profiles.

- About Recording Profile setup, page 731
- Recording profile deletion, page 731
- Recording profile settings, page 732

About Recording Profile setup

In Cisco Unified Communications Manager Administration, use the Device > Phone > Recording Profile menu path to configure recording profiles.

To provision line appearances of agents for call recording, you create one or more call recording profiles. You then select a recording profile for a line appearance.

Recording profile deletion

You cannot delete a recording profile that a line appearance uses. To find out which line appearances are using the recording profile, choose Dependency Records from the Related Links drop-down list box that is on the Recording Profile Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message. If you try to delete a recording profile that is in use, Cisco Unified Communications Manager displays a message. Before deleting a recording profile that is currently in use, you must perform either or both of the following tasks:

- Assign a different recording profile to any line appearances that are using the recording profile that you want to delete.
- Delete the line appearances that are using the recording profile that you want to delete.

Related Topics

Access dependency records, on page 874
Recording profile settings

The following table describes the recording profile settings.

Table 109: Recording profile settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the recording profile.</td>
</tr>
<tr>
<td>Recording Calling Search Space</td>
<td>From the drop-down list box, choose the calling search space that contains the partition of the route pattern that is associated with the SIP trunk that is configured for the recorder.</td>
</tr>
<tr>
<td>Recording Destination Address</td>
<td>Enter the directory number (DN) or the URL of the recorder that associates with this recording profile.</td>
</tr>
<tr>
<td></td>
<td>This field allows any characters except the following characters: double quotation marks (&quot;), back quote (‘), and space ( ).</td>
</tr>
</tbody>
</table>

Related Topics

Recording Profile setup, on page 731
SIP normalization script setup

This chapter provides information about Cisco Unified Communications Manager SIP normalization script configuration.

- About SIP normalization script setup, page 733
- SIP normalization script deletion, page 734
- SIP normalization script settings, page 734
- Import SIP normalization script, page 737

About SIP normalization script setup

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > SIP Normalization Script menu path to configure SIP normalization and transparency scripts.

SIP trunks can connect to a variety of endpoints, including PBXs, gateways, and service providers. Each of these endpoints implements the SIP protocol a bit differently, causing a unique set of interoperability issues. To normalize messages per trunk, Cisco Unified Communications Manager allows you to add or update scripts to the system and then associate them with one or more SIP trunks. The normalization scripts that you create allow you to preserve, remove, or change the contents of any SIP headers or content bodies, known or unknown.

Transparency refers to the ability to pass information from one call leg to the other. REFER transparency allows Cisco Unified Communications Manager to pass on REFER requests to another endpoint rather than acting on them. REFER transparency is key in call center applications, where the agent sending the REFER (initiating the transfer) resides in a geographic area remote from both of the other call parties.

After you configure a script in Cisco Unified Communications Manager, you associate the script with a SIP trunk by configuring the Normalization Script fields in the Trunk Configuration window. You can only associate one script per trunk, but you can associate the same script to multiple trunks.

SIP normalization scripts configuration tips

You cannot edit the refer-passthrough script. If you want to use the content of the refer-passthrough script in a custom script, display the script in the SIP Normalization Script window. Copy the information from the Content field, click the Add New button to create a new script record, and paste the information from the refer-passthrough script into the new record.
SIP normalization script deletion

You cannot delete the refer-passthrough script.

SIP normalization script settings

The following table describes the SIP normalization script settings.

Table 110: SIP normalization script settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique identifier for the script. The name can comprise up to 50</td>
</tr>
<tr>
<td></td>
<td>alphanumeric characters and can contain any combination of spaces, periods</td>
</tr>
<tr>
<td></td>
<td>(.), hyphens (-), and underscore characters (_).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the script.</td>
</tr>
<tr>
<td>Content</td>
<td>This field displays the content of the imported script. You can edit the</td>
</tr>
<tr>
<td></td>
<td>script in this text box.</td>
</tr>
</tbody>
</table>
### Script Execution Error Recovery Action

Choose the action that you want the system to perform when an execution error gets detected while executing a script message handler.

An execution error can occur due a number of issues, such as a script invokes one of the Cisco SIP Message APIs but passes in the wrong number of arguments, or a script passes a nil string to a string library API.

When an execution error gets detected, the system automatically exits the message handler at the point of the failure, restores the message to its original content prior to executing the message handler (in other words, performs message rollback), and continues as if the message handler was never invoked.

After the automatic error message handling, the system performs the action that you choose from the drop-down list box:

- **SIP Message Rollback Only**—(Default) The script continues to execute for subsequent messages.
- **SIP Disable Script**—Cisco Unified Communications Manager closes the script and does not execute it for subsequent messages. The Lua state remains closed and the system reclaims all of the memory. You must manually reset the trunk to re-enable the script.
- **SIP Reset Script**—Cisco Unified Communications Manager closes and immediately reloads the script. When the script is closed, the Lua state is closed and the system reclaims all of the memory. Any state that the script maintains is lost. After the script reloads, Cisco Unified Communications Manager automatically uses the script for subsequent messages.
- **SIP Script Reset Trunk**—The system immediately resets the trunk, which affects existing calls. Cisco Unified Communications Manager closes the script while the trunk resets. After the trunk restarts, Cisco Unified Communications Manager automatically reopens the script.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script Execution Error</td>
<td>Choose the action that you want the system to perform when an execution error gets detected while executing a script message handler. An execution error can occur due to a number of issues, such as a script invokes one of the Cisco SIP Message APIs but passes in the wrong number of arguments, or a script passes a nil string to a string library API. When an execution error gets detected, the system automatically exits the message handler at the point of the failure, restores the message to its original content prior to executing the message handler (in other words, performs message rollback), and continues as if the message handler was never invoked. After the automatic error message handling, the system performs the action that you choose from the drop-down list box: • <strong>SIP Message Rollback Only</strong>—(Default) The script continues to execute for subsequent messages. • <strong>SIP Disable Script</strong>—Cisco Unified Communications Manager closes the script and does not execute it for subsequent messages. The Lua state remains closed and the system reclaims all of the memory. You must manually reset the trunk to re-enable the script. • <strong>SIP Reset Script</strong>—Cisco Unified Communications Manager closes and immediately reloads the script. When the script is closed, the Lua state is closed and the system reclaims all of the memory. Any state that the script maintains is lost. After the script reloads, Cisco Unified Communications Manager automatically uses the script for subsequent messages. • <strong>SIP Script Reset Trunk</strong>—The system immediately resets the trunk, which affects existing calls. Cisco Unified Communications Manager closes the script while the trunk resets. After the trunk restarts, Cisco Unified Communications Manager automatically reopens the script.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Resource Error</td>
<td>Choose the action that you want Cisco Unified Communications Manager to take when a script aborts during execution because Memory Threshold and Lua Instruction Threshold values were exceeded. Resource errors can occur when the script is loading, initializing, or executing a message handler. If the script fails to load or initialize, it is immediately disabled. The configured System Resource Error Recovery Action does not apply to load and initialization errors. This action applies only to execution errors. Execution errors occur only while executing message handlers. When a resource error occurs while a script executes a message handler, the system automatically exits the message handler at the point of the failure, restores the message to its original content prior to executing the message handler (in other words, performs message rollback), and continues as if the message handler was never invoked. After the automatic error message handling, the system performs the action that you choose from the drop-down list box:</td>
</tr>
<tr>
<td>Recovery Action</td>
<td>• SIP Disable Script—(Default) The script closes and does not execute for subsequent messages. The Lua state remains closed and the system reclaims all of the memory. You must manually reset the trunk to re-enable the script. • SIP Reset Script—The script closes and then immediately reloads. When the script closes, the Lua state closes and the system reclaims all of the memory. Any state that the script maintains is lost. After the script reloads, Cisco Unified Communications Manager automatically uses the script for subsequent messages. • SIP Script Reset Trunk—The system immediately resets the trunk, which affects existing calls. The script closes while the trunk resets. After the trunk restarts, the script reopens automatically.</td>
</tr>
<tr>
<td>Memory Threshold</td>
<td>Enter the memory threshold value in kilobytes. You must enter an integer into this field. If memory usage exceeds 80 percent of this value, the SIPNormalizationScriptResourceWarning resource warning alarm gets generated. The script continues to execute until the memory usage exceeds 100 percent of this value. If memory usage exceeds 100 percent during script loading or initialization, a script error alarm gets generated, and the script gets closed and disabled. If memory usage exceeds 100 percent during script execution, a script error alarm gets generated, and Cisco Unified Communications Manager performs the action that the System Resource Error Recovery Action field specifies. For example, if you enter 50 kilobytes into this field, the warning alarm gets generated if the script exceeds 40 kilobytes. The script continues to run until memory usage exceeds 50 kilobytes. The default value specifies 50 kilobytes.</td>
</tr>
</tbody>
</table>
This field specifies the maximum number of Lua instructions that a given message handler is allowed to invoke. If a script exceeds 50 percent of this value, a resource warning alarm generates. The script continues to execute until the script exceeds 100 percent of this value.

If the script exceeds 100 percent of the Lua Instruction Threshold value during script loading or initialization script, the SIPNormalizationScriptResourceWarning resource warning alarm gets generated and Cisco Unified Communications Manager closes and disables the script.

If the script exceeds 100 percent of the Lua Instruction Threshold value during script execution, the SIPNormalizationScriptResourceWarning alarm gets generated and Cisco Unified Communications Manager performs the action that the System Resource Error Recovery Action field specifies.

For example, if you enter 1000 in this field, a warning alarm gets generated if the script exceeds 500 instructions. The script continues to run until it exceeds 1000 instructions.

The default value specifies 1000 instructions per message handler invocation.

Click this button to shut down, then restart, the internal trunk device or devices with which this script associates.

Click this button to import a script.

In the Import File popup window that opens, search for the file by clicking the Browse... button to the right of the Import File field. Use the File Upload popup window to navigate to the file to you want to upload. After you find the file, click the desired filename and click Open. The path to the chosen script file displays in the Import File field of the Import File popup window. To upload the specified script file, click Import File. To close the Import File popup window without taking any action, click Close.

After the script file uploads, the Status area of the Import File window tells you the result of the upload. The contents of the script file display in the Content field.

Related Topics

SIP normalization script setup, on page 733

Import SIP normalization script

Perform the following procedure to import a SIP normalization script into Cisco Unified Communications Manager.

Procedure

Step 1 Choose Device > Device Settings > SIP Normalization Script.
The Find and List SIP Normalization window displays.

**Step 2** Perform one of the followings tasks:

a) To add a new script instance, click the Add New button. The SIP Normalization Script Configuration window displays.

b) To update an existing script instance, locate the appropriate script instance, and click the name of the script that you want to update.

**Step 3** To import a script, click the Import File button. The Import File dialog box displays.

**Step 4** Click the Browse button to locate the file that you want to import, and click the Open button.

**Step 5** Click the Import File button. The contents of the script file display in the Content field.

**Step 6** Modify any of the necessary fields on the window.

**Step 7** Click Save and then click Reset.

**Related Topics**

- SIP normalization script setup, on page 733
- About SIP normalization script setup, on page 733
Other device menu options

This chapter provides brief descriptions of selected Device menu options that other documents describe in greater detail. A pointer to the document that contains more details is provided for each Device menu option.

- Remote destination setup, page 739
- Remote destination profile setup, page 739

Remote destination setup

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Remote Destination menu path to configure remote destinations.

The Cisco Unified Mobility Mobile Connect feature allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and mobile phone. Mobile Voice Access is the associated integrated voice response (IVR) system, which allows users to turn Mobile Connect on or off and to initiate calls from a mobile phone or other remote phone as if the call were initiated from the desktop phone.

Remote destinations represent the mobile (or other) phones that are able to accept transfers from the user desktop phone and can be used to initiate calls using Mobile Voice Access.

For more information on Mobile Connect, Mobile Voice Access, and other Cisco Unified Mobility features, as well as how to configure remote destinations, see the Cisco Unified Communications Manager Features and Services Guide.

Remote destination profile setup

In Cisco Unified Communications Manager Administration, use the Device > Device Settings > Remote Destination Profile menu path to configure remote destination profiles.

Mobile Connect allows users to manage business calls using a single phone number and pick up in-progress calls on the desktop phone and cellular phone. Mobile Voice Access is the associated integrated voice response (IVR) system, which allows users to turn Mobile Connect on or off and to initiate calls from a cellular phone or other remote phone as if the call were initiated from the desktop phone.

A user remote destination profile contains the parameters that apply to all the remote destinations (cellular or other phones) available for in-progress call transfers and initiation of calls by way of Mobile Voice Access.
For more information on Mobile Connect and Mobile Voice Access and how to configure remote destination profiles, see the *Cisco Unified Communications Manager Features and Services Guide*.
PART VII

Application setup

• Cisco Unified Communications Manager Assistant Configuration Wizard, page 743
• Plug-in setup, page 745
CHAPTER 85

Cisco Unified Communications Manager Assistant Configuration Wizard

With the Cisco Unified Communications Manager Assistant Configuration Wizard, Cisco Unified Communications Manager Assistant configuration takes less time and eliminates errors. The partitions, calling search spaces, route point, and translation pattern automatically get created when the administrator successfully runs and completes the configuration wizard. The wizard also creates BAT templates for the Cisco Unified Communications Manager Assistant manager phone, the Cisco Unified Communications Manager Assistant 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.

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.

For more information on how to use the Cisco Unified Communications Manager Assistant Configuration Wizard, see the Cisco Unified Communications Manager Features and Services Guide.
Plug-in setup

This chapter provides information to install and update Application plug-ins for the Cisco Unified Communications Manager.

- Update plugin URL settings, page 745
- Install plug-ins, page 746
- Update plugin URL, page 746

Update plugin URL settings

Application plug-ins extend the functionality of Cisco Unified Communications Manager. For example, the JTAPI plug-in allows a computer to host applications that access the Cisco Unified Communications Manager via the Java Telephony Application Programming Interface (JTAPI).

The following table describes the Update Plugin URL configuration settings.

Table 111: Update Plugin URL configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Settings</td>
<td></td>
</tr>
<tr>
<td>Plugin Name</td>
<td>The plug-in name automatically displays.</td>
</tr>
<tr>
<td>URL</td>
<td>The existing URL automatically displays.</td>
</tr>
<tr>
<td>Custom URL</td>
<td>Use only alphanumeric characters for the custom URL.</td>
</tr>
<tr>
<td>Show Plugin on User Option Pages</td>
<td>Check this check box to show the plug-in on the user option window.</td>
</tr>
</tbody>
</table>
Install plug-ins

Perform the following procedure to install any plug-in.

**Tip**
After Cisco Unified Communications Manager upgrades, you must reinstall all plug-ins except the Cisco CDR Analysis and Reporting plug-in.

**Tip**
Before you install any plug-ins, disable all intrusion detection or antivirus services that run on the server where you plan to install the plug-in.

**Procedure**

**Step 1**
Choose Application > Plugins.
The Find and List Plugins 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.
To filter or search records
a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) From the third drop-down list box, select Application Menu, Installation, User Menu, or Telecaster Menu.
d) 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** To reverse the sort order, click the up or down arrow, if available, in the list header.

**Step 4**
Click Download for the plug-in you want to install.

Update plugin URL

During the Cisco Unified Communications Manager install process, records that are added to the Plugins table specify the URLs that the Administration applications use to build the Application drop-down menu. The domain name server (DNS) provides the basis for the URL that is constructed at installation time. If the DNS changes, the URL does not get updated.

Perform the following procedure to update the URL of the Plugin URL.
Procedure

**Step 1** Choose Application > Plugins. The Find and List Plugins window displays. Display the list of available plug-ins.

**Step 2** Click the Plugin name that you want to update. The Update Plugin URL window displays.

**Step 3** Enter the update plugin URL configuration settings.

**Step 4** Click the Save icon that displays in the tool bar in the upper, left corner of the window (or click the Save button that displays at the bottom of the window) to update and save the URL.

**Related Topics**

- Update plugin URL settings, on page 745
- Install plug-ins, on page 746
Update plugin URL
PART VIII

User management setup

• Credential policy default setup, page 751
• Credential policy setup, page 755
• Application user setup, page 759
• End user setup, page 771
• Role setup, page 787
• Access control group setup, page 791
• End user phone addition, page 799
• UC service setup, page 803
• Service profile setup, page 815
• Universal device template setup, page 821
• Feature group template setup, page 857
• Quick user and phone addition, page 861
• Other user management menu options, page 867
CHAPTER 87

Credential policy default setup

This chapter provides information to configure credential policies.

- About credential policy default setup, page 751
- Assign and set up credential policy defaults, page 753

About credential policy default setup

In Cisco Unified Communications Manager Administration, use the User Management > Credential Policy Default menu path to configure credential policy defaults.

This chapter describes how to assign default credential policies to a credential group.

The Credential Policy Default window provides options to change the default credential policy assignment for a user and credential type (for example, end user PINs). At installation, Cisco Unified Communications Manager assigns the system Default Credential Policy to end user passwords, end user PINs, and application user passwords. The system applies the application password that you configured at installation to all application users. You can assign a new default credential policy and configure new default credentials after installation.

Credential policy defaults configuration tips

The system provides the default credential policy to facilitate installs and upgrades. The default credential policy settings in Table 112: Credential policy default settings, on page 752 differ from the credential policy defaults settings that are used to add a new credential policy.

Note

The system does not support empty (null) credentials. If your system uses LDAP authentication, you must configure end user default credentials immediately after installation, or logins will fail.

You can also assign a new user credential policy, manage user authentication events, or view credential information for a user in the user configuration windows.

Related Topics

- Manage application user credential information, on page 767
- Manage end user credential information, on page 782
**Credential policy default settings**

The following table describes the credential policy default settings.

**Table 112: Credential policy default settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential User</td>
<td>This field displays the user type for the policy that you selected in the Find and List Credential Policy Defaults window. You cannot change this field.</td>
</tr>
<tr>
<td>Credential Type</td>
<td>This field displays the credential type for the policy that you selected in the Find and List Credential Policy Defaults window. You cannot change this field.</td>
</tr>
<tr>
<td>Credential Policy</td>
<td>Choose a credential policy default for this credential group. The list box displays the predefined Default Credential Policy and any credential policies that you created.</td>
</tr>
<tr>
<td>Change Credential</td>
<td>Enter up to 127 characters to configure a new default credential for this group.</td>
</tr>
<tr>
<td>Confirm Credential</td>
<td>For verification, reenter the login credential that you entered in the Change Credential field.</td>
</tr>
<tr>
<td>User Cannot Change</td>
<td>Check this check box to block users that are assigned this policy from changing this credential. You cannot check this check box when User Must Change at Next Login is checked. The default setting for this check box specifies unchecked.</td>
</tr>
<tr>
<td>User Must Change at Next Login</td>
<td>Check this check box to require users that are assigned this policy to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when the User Cannot Change check box is checked. The default setting for this check box specifies checked.</td>
</tr>
<tr>
<td>Does Not Expire</td>
<td>Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If this check box is checked, the user can still change this credential at any time. When this check box is unchecked, the expiration setting in the associated credential policy applies. The default setting for this check box specifies unchecked.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Credential policy default setup](#), on page 751
- [Credential policy setup](#), on page 755
Assign and set up credential policy defaults

This section describes how to assign a new credential policy and new default credentials to a credential group. At installation, the system assigns a default credential policy to the credential groups.

---

**Note**

Upgrades from 5.x releases automatically migrate application and end user passwords and PINs.

---

**Before You Begin**

To assign a default credential policy other than the predefined Default Credentials Policy, you must first create the policy.

---

**Procedure**

**Step 1** Choose User Management > Credential Policy Default. The Find and List Find and List Credential Policy Defaults window displays.

**Step 2** Click the list item to change. The Credential Policy Default Configuration window displays with the current settings.

**Step 3** Enter the appropriate settings, as described in Table 112: Credential policy default settings, on page 752, using these guidelines:

- a) To change the applied credential policy, select the policy from the drop-down list box.
- b) To change the default credential, enter and confirm the new credential in the appropriate fields.
- c) To change credential requirements, check or uncheck the appropriate check boxes.

**Step 4** Click the Save button or the Save icon.

---

**What to Do Next**

You can assign a new user credential policy, manage user authentication events, view credential information for a user, or configure a unique password for the user.

The Bulk Administration Tool (BAT) allows administrators to define common credential parameters, such as passwords and PINs, for a group of users in the BAT User Template. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

End users can change PINs at the phone user pages; end users can change passwords at the phone user pages when LDAP authentication is not enabled. See the documentation for your Cisco Unified IP Phone for more information.

**Related Topics**

- Credential policy setup, on page 755
- Change application user password, on page 767
- Manage application user credential information, on page 767
- Change end user password, on page 781
- Change end user PIN, on page 781
- Manage end user credential information, on page 782
Assign and set up credential policy defaults
Credential policy setup

This chapter provides information to configure credential policies.

• About credential policy setup, page 755
• Credential policy deletion, page 756
• Credential policy settings, page 757

About credential policy setup

In Cisco Unified Communications Manager Administration, use the User Management > Credential Policy menu path to configure credential policies.

The Credential Policy Configuration window in Cisco Unified Communications Manager Administration allows you to configure credential policies to secure user accounts.

A policy comprises a set of rules that controls access to a system or network resource. A credential policy defines password requirements and account lockouts for user accounts. Credential policies that are assigned to user accounts control the authentication process in Cisco Unified Communications Manager. After you add a credential policy, you can assign the new policy as the default policy for a credential type or to an individual application or end user.

At installation, Cisco Unified Communications Manager assigns a static credential policy to end user PINs and to application and end user passwords. The policy contains settings for failed login resets, lockout durations, expiration periods, and credential requirements. The Credential Policy Configuration window allows you to configure new credential policies for your system or site. You cannot change the static policy.

Credential policies configuration tips

The system provides trivial credential checks to disallow credentials that are easily hacked. You enable trivial credential checks by checking the Check for Trivial Passwords check box in the Credential Policy Configuration window.

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets the following criteria:

• Must contain three of the four allowable characteristics: uppercase character, lowercase character, number, symbol.
• Must not use a character or number more than three times consecutively.
• Must not repeat or include the alias, username, or extension.
• Cannot consist of consecutive characters or numbers (for example, passwords such as 654321 or ABCDEFG)

PINs can contain digits (0-9) only. A non-trivial PIN meets the following criteria:
• Must not use the same number more than two times consecutively.
• Must not repeat or include the user extension or mailbox or the reverse of the user extension or mailbox.
• Must contain three different numbers; for example, a PIN such as 121212 is trivial.
• Must not match the numeric representation (that is, dial by name) for the first or last name of the user.
• Must not contain groups of repeated digits, such as 408408, or patterns that are dialed in a straight line on a keypad, such as 2580, 159, or 753.

Tip
You cannot modify the system Default Credential Policy.

Next Steps
You can assign the new credential policy as a default policy for a credential type, or to individual users.

Related Topics
Assign and set up credential policy defaults, on page 753
Manage application user credential information, on page 767
Manage end user credential information, on page 782

Credential policy deletion

Note
You cannot delete a credential policy if it is assigned as the default policy for end user passwords, end user PINS, or application user passwords.

To find out which default policies use the credential policy, choose Dependency Records from the Related Links drop-down list box in the Credential Policy Configuration window and click Go.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records. The message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a credential policy that is in use, a message displays. To delete a credential policy that is currently in use, you must either choose a different credential policy for the user or create and assign a new policy.

Related Topics
About credential policy setup, on page 755
**Credential policy settings**

The following table describes the credential policy settings.

*Table 113: Credential policy settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Specify the credential policy name. Enter up to 64 characters, except for quotation marks. Do not enter tab.</td>
</tr>
<tr>
<td>Failed Logon / No Limit for Failed Logons</td>
<td>Specify the number of allowed failed login attempts. When this threshold is reached, the system locks the account. Enter a number in the range 1-100. To allow unlimited failed logins, enter 0 or check the No Limit for Failed Logons check box. Uncheck the check box to enter a value greater than 0. The default setting specifies 3.</td>
</tr>
<tr>
<td>Reset Failed Logon Attempts Every</td>
<td>Specify the number of minutes before the counter is reset for failed login attempts. After the counter resets, the user can try logging in again. Enter a number in the range 1-120. The default setting specifies 30.</td>
</tr>
<tr>
<td>Lockout Duration / Administrator Must Unlock</td>
<td>Specify the number of minutes an account remains locked when the number of failed login attempts exceeds the specified threshold. Enter a number in the range 1-1440. Enter 0 or check the Administrator Must Unlock check box, so accounts will remain locked until an administrator manually unlocks them. Uncheck the check box to enter a value greater than 0. The default setting specifies 30.</td>
</tr>
<tr>
<td>Minimum Duration Between Credential Changes</td>
<td>Specify the number of minutes that are required before a user can change credentials again. Enter 0 to allow a user to change credentials at any time. Uncheck the check box to enter a value greater than 0. The default setting specifies 0.</td>
</tr>
<tr>
<td>Credential Expires After / Never Expires</td>
<td>Specify the number of days before a credential will expire. Enter a number in the range 1-365. To allow credentials to never expire, enter 0 or check the Never Expires check box. Uncheck the check box to enter a value greater than 0. Use the 0 option for low-security accounts or multiple user accounts, for example. The default setting specifies 180.</td>
</tr>
<tr>
<td>Minimum Credential Length</td>
<td>Specify the minimum length for user credentials (password or PIN). Do not enter 0 because blank passwords are not allowed. The default setting specifies 8. The minimum setting must equal at least 1.</td>
</tr>
</tbody>
</table>
### Field Description

**Stored Number of Previous Credentials**
Specify the number of previous user credentials to store. This setting prevents a user from configuring a recently used credential that is saved in the user list. Enter a number in the range 0-25. If no previous credentials should be stored, enter 0. The default setting specifies 12.

**Inactive Days Allowed**
Specify the number of days that a password can remain inactive before the account gets locked. Enter a number in the range 0-5000. The default setting specifies 0.

**Expiry Warning Days**
Enter a number in the range 0-90 to specify the number of days before a user password expires to start warning notifications. The default setting specifies 0.

**Check for Trivial Passwords**
Check this check box to require the system to disallow credential that are easily hacked, such as common words, repeated character patterns, and so on. The default setting checks the check box.

### Related Topics

- Credential policy setup, on page 755
CHAPTER 89

Application user setup

This chapter provides information on managing application user information.

- About application user setup, page 759
- Add application user, page 760
- Application user deletion, page 761
- Application user settings, page 761
- Add administrator user to Cisco Unity or Cisco Unity Connection, page 765
- Change application user password, page 767
- Manage application user credential information, page 767
- Credential settings and fields, page 768
- Associate devices to application users, page 769

About application user setup

In Cisco Unified Communications Manager Administration, use the User Management > Application User menu path to configure application users.

The Application User Configuration window in Cisco Unified Communications Manager Administration allows the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager application users.

Application users configuration tips

Click Add New to set up a new application user. Complete the fields in the Application User Configuration window to configure settings for the application user. For details, see Application user settings, on page 761.

Note

Installation provides a set of default application users for Cisco Unified Communications Manager.
If you are adding an administrator account for Cisco Unity or Cisco Unity Connection, you must use the same user name and password that you defined in Cisco Unity and Cisco Unity Connection Administration. The user ID provides authentication between Cisco Unity or Cisco Unity Connection and Cisco Unified Communications Manager Administration. See the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity or Cisco Unity Connection.

You can configure a Cisco Unified Communications Manager Administration application user as a Cisco Unity or Cisco Unity Connection user by using the Create a Cisco Unity Application User option in the Application User Configuration window. You can then configure any additional settings in Cisco Unity or Cisco Unity Connection Administration.

To show the user privilege report for this application user, from the Related Links drop-down list box, choose User Privilege Report and click Go.

The User Privilege window displays for this application user.

After you display the user privilege report for this application user, you can return to the Application User Configuration window for this application user. From the Related Links drop-down list box in the User Privilege window, choose Back to Application User and click Go.

Next steps
You can associate devices with this application user, manage the application user credentials, and add an administrator user to Cisco Unity or Cisco Unity Connection.

Related Topics
- Add administrator user to Cisco Unity or Cisco Unity Connection, on page 765
- Manage application user credential information, on page 767
- Associate devices to application users, on page 769
- View user roles, access control groups, and permissions, on page 797

Add application user

To add an application user, perform the following steps:

Procedure

Step 1 In Cisco Unified CM Administration, choose User Management > Application User.
Step 2 Click Add New.
Step 3 Complete the fields in the Application User Configuration window and click Save. For field descriptions, see Application user settings, on page 761.
Step 4 Click Save.

What to Do Next
To associate a device to an application user, see Associate devices to application users, on page 769.
Application user deletion

Before deleting the application user, determine whether the devices or profiles that are associated with the end user need to be removed or deleted.

You can view the profiles and permissions that are assigned to the application user from the CAPF Information and Permissions Information areas of the Application User Configuration window. You can also choose Dependency Records from the Related Links drop-down list box in the Application User Configuration window. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Next steps

If this user is configured in Cisco Unity or Cisco Unity Connection, the user association to Cisco Unified Communications Manager is broken when you delete the user in Cisco Unified Communications Manager Administration. You can delete the orphaned user in Cisco Unity or Cisco Unity Connection Administration. See the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection for more information. See the applicable System Administration Guide for Cisco Unity for more Cisco Unity information.

Related Topics

Access dependency records, on page 874

Application user settings

The following table describes the application user settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application User Information</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>Enter a unique application user identification name. Cisco Unified Communications Manager allows you to modify an existing user ID (provided synchronization with the LDAP server is not enabled). You can enter the following characters: alphanumeric (a-zA-Z0-9), dash(-), underscore(_), or space( ).</td>
</tr>
<tr>
<td>Password</td>
<td>Enter alphanumeric or special characters for the application user password. You must enter at least the minimum number of characters that are specified in the assigned credential policy. <strong>Note</strong> Do not use special characters when you create an AXL password for an application user.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the user password again.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Digest Credentials</td>
<td>Enter a string of alphanumeric characters. Cisco Unified Communications Manager uses the digest credentials that you specify here to validate the SIP user agent response during a challenge to the SIP trunk. For information on digest authentication, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Confirm Digest Credentials</td>
<td>To confirm that you entered the digest credentials correctly, enter the credentials in this field.</td>
</tr>
<tr>
<td>Edit Credential</td>
<td>The Edit Credential button displays after you add this user to the database. Click this button to manage credential information for this user.</td>
</tr>
<tr>
<td>Presence Group</td>
<td>Configure this field with the Presence feature.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. The Standard Presence group gets configured at installation. Presence groups 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 <em>Cisco Unified Communications Manager Features and Services Guide</em> for information about configuring permissions between groups.</td>
</tr>
<tr>
<td>Accept Presence Subscription</td>
<td>Configure this field with the Presence feature for presence authorization. If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization. Check this check box to authorize Cisco Unified Communications Manager to accept presence requests that come from this SIP trunk application user. If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk. For more information on authorization, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Accept Out-of-Dial REFER      | If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization.  
Check this check box to authorize Cisco Unified Communications Manager to accept Out-of-Dial REFER requests that come from this SIP trunk application user. For example, to use SIP-initiated transfer features and other advanced transfer-related features, you must authorize Cisco Unified Communications Manager to accept incoming Out-of-Dial REFER requests for this application user.  
If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk.  
For more information on authorization, see the *Cisco Unified Communications Manager Security Guide*. |
| Accept Unsolicited Notification | If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization.  
Check this check box to authorize Cisco Unified Communications Manager to accept unsolicited notifications that come from this SIP trunk application user. For example, to provide MWI support, you must authorize Cisco Unified Communications Manager to accept incoming unsolicited notifications for this application user.  
If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager sends a 403 error message to the SIP user agent that is connected to the trunk.  
For more information on authorization, see the *Cisco Unified Communications Manager Security Guide*. |
### Accept Replaces Header

If you enabled application-level authorization in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified Communications Manager performs application-level authorization.

Check this check box to authorize Cisco Unified CM to accept header replacements in messages from this SIP trunk application user. For example, to transfer an external call on a SIP trunk to an external device or party, as in attended transfer, you must authorize Cisco Unified CM to accept SIP requests with replaces header in REFERS and INVITES for this application user.

If you check this check box in the Application User Configuration window and do not check the Enable Application Level Authorization check box in the SIP Trunk Security Profile Configuration applied to the trunk, Cisco Unified CM sends a 403 error message to the SIP user agent that is connected to the trunk.

For more information on authorization, see the *Cisco Unified Communications Manager Security Guide*.

### Device Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Available Devices | This list box displays the devices that are available for association with this application user. To associate a device with this application user, select the device and click the Down arrow below this list box. If the device that you want to associate with this application user does not display in this pane, click one of these buttons to search for other devices:  
  • Find more Phones—Click this button to find more phones to associate with this application user. The Find and List Phones window displays to enable a phone search.  
  • Find more Route Points—Click this button to find more route points to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search.  
  • Find more Pilot Points—Click this button to find more pilot points to associate with this application user. The Find and List Pilot Points window displays to enable a pilot point search. |
| Controlled Devices | This field lists the devices that are associated with the application user. To remove a device, select the device name and click the Up arrow above this list box. To add a device, select a device in the Available Devices list box and click the Down arrow. |

### CAPF Information
Add administrator user to Cisco Unity or Cisco Unity Connection

The Create Cisco Unity Application User link in the Application Configuration window allows you to add a user as an administrator user to Cisco Unity or Cisco Unity Connection. With this method, you configure the application user in Cisco Unified Communications Manager Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration.
If you are integrating Cisco Unified Communications Manager with Cisco Unity Connection 7.x, you can use the import feature that is available in Cisco Unity Connection 7.x instead of performing the procedure that is described in this section. For information on how to use the import feature, see the User Moves, Adds, and Changes Guide for Cisco Unity Connection 7.x.

The Create Cisco Unity User link displays only if you install and configure the appropriate Cisco Unity or Cisco Unity Connection software. See the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity or the applicable Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection.

**Before You Begin**

Ensure that you have defined an appropriate template for the user that you plan to push to Cisco Unity or Cisco Unity Connection. For Cisco Unity Connection users, see the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. For Cisco Unity users, see the System Administration Guide for Cisco Unity.

**Procedure**

**Step 1** Find the application user.

**Step 2** From the Related Links drop-down list box, choose the Create Cisco Unity Application User link and click Go. The Add Cisco Unity User dialog box displays.

**Step 3** From the Application Server drop-down list box, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity or Cisco Unity Connection user and click Next.

**Step 4** From the Application User Template drop-down list box, choose the template that you want to use.

**Step 5** Click Save. The administrator account gets created in Cisco Unity or Cisco Unity Connection. The link in Related Links changes to Edit Cisco Unity User in the Application User Configuration window. You can now view the user that you created in Cisco Unity Administration or Cisco Unity Connection Administration.

**Note** When the Cisco Unity or Cisco Unity Connection user is integrated with the Cisco Unified CM Application User, you cannot edit fields such as Alias (User ID in Cisco Unified Communications Manager Administration), First Name, Last Name, Extension (Primary Extension in Cisco Unified Communications Manager Administration), and so on, in Cisco Unity Administration or Cisco Unity Connection Administration. You can only update these fields in Cisco Unified Communications Manager Administration.

**Note** Cisco Unity and Cisco Unity Connection monitor the synchronization of data from Cisco Unified Communications Manager. You can configure the sync time in Cisco Unity Administration or Cisco Unity Connection Administration on the Tools menu. For Cisco Unity Connection, see the User Moves, Adds, and Changes Guide for Cisco Unity Connection for more information. For Cisco Unity, see the System Administration Guide for Cisco Unity.

**Related Topics**

Application user setup, on page 759
Change application user password

Use the following procedure to change an application user password.

Procedure

**Step 1**  Find the application user whose password you want to change.
The Application User Configuration window displays information about the chosen application user.

**Step 2**  In the Password field, double-click the existing, encrypted password and enter the new password.

**Step 3**  In the Confirm Password field, double-click the existing, encrypted password and enter the new password again.

**Step 4**  Click Save.

Related Topics

- Application user setup, on page 759

Manage application user credential information

Use the following procedure to change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an application user. You can edit user credentials only after the user exists in the database.

You cannot save settings in the user Credential Configuration window that conflict with the assigned credential policy. For example, if the policy has the Never Expires check box checked, you cannot uncheck and save the Does Not Expire check box in the user Credential Configuration window. You can, however, set a different credential expiration for the user, including Does Not Expire, if the Never Expires policy setting is not checked; the user setting overrides the policy setting.

You cannot change settings in the user Credential Configuration window that conflict with other settings in the user Credential Configuration window. For example, if the User Cannot Change box is checked, you cannot check the User Must Change at Next Login check box.

The Credential Configuration window provides approximate event times; the system updates the form at the next authentication query or event.

**Before You Begin**

Create the application user in the database.

**Procedure**

**Step 1**  Use the Finding an Application User window to find the application user configuration (User Management > Application User).
The Application User Configuration window displays the configuration information.
Step 2  
To change or view password information, click the Edit Credential button next to the Password field. The user Credential Configuration window displays.

Step 3  
View the credential data for the user or enter the appropriate settings, as described in Table 115: Application user and end user credential settings and fields, on page 768.

Step 4  
If you have changed any settings, click Save.

## Credential settings and fields

The following table describes credential settings for application users and end users. These settings do not apply to application user or end user digest credentials.

### Table 115: Application user and end user credential settings and fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked By Administrator</td>
<td>Check this check box to lock this account and block access for this user.</td>
</tr>
<tr>
<td></td>
<td>Uncheck this check box to unlock the account and allow access for this user.</td>
</tr>
<tr>
<td></td>
<td>Use this check box when the credential policy specifies that an Administrator Must Unlock this account type after an account lockout.</td>
</tr>
<tr>
<td>User Cannot Change</td>
<td>Check this check box to block this user from changing this credential. Use this option for group accounts.</td>
</tr>
<tr>
<td></td>
<td>You cannot check this check box when User Must Change at Next Login check box is checked.</td>
</tr>
<tr>
<td>User Must Change at Next Login</td>
<td>Check this check box to require the user to change this credential at next login. Use this option after you assign a temporary credential.</td>
</tr>
<tr>
<td></td>
<td>You cannot check this check box when User Cannot Change check box is checked.</td>
</tr>
<tr>
<td>Does Not Expire</td>
<td>Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts.</td>
</tr>
<tr>
<td></td>
<td>If checked, the user can still change this credential at any time. When the check box is unchecked, the expiration setting in the associated credential policy applies.</td>
</tr>
<tr>
<td></td>
<td>You cannot uncheck this check box if the policy setting specifies Does Not Expire.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reset Hack Count</td>
<td>Check this check box to reset the hack count for this user and clear the Time Locked Due to Failed Login Attempts field. The hack count increments whenever authentication fails for an incorrect credential. If the policy specifies No Limit for Failed Logons, the hack count always specifies 0.</td>
</tr>
<tr>
<td>Authentication Rule</td>
<td>Select the credential policy to apply to this user credential.</td>
</tr>
<tr>
<td>Time Last Changed</td>
<td>This field displays the date and time of the most recent credential change for this user.</td>
</tr>
<tr>
<td>Failed Logon Attempts</td>
<td>This field displays the number of failed login attempts since the last successful login, since the administrator reset the hack count for this user credential, or since the reset failed login attempts time expired.</td>
</tr>
<tr>
<td>Time of Last Field Logon</td>
<td>This field displays the date and time for the most recent failed login attempt for this user credential.</td>
</tr>
<tr>
<td>Time Locked by Administrator</td>
<td>This field displays the date and time that the administrator locked this user account. This field goes blank after the administrator unlocks the credential.</td>
</tr>
<tr>
<td>Time Locked Due to Failed</td>
<td>This field displays the date and time that the system last locked this user account due to failed login attempts. Time of hack lockout gets set whenever failed login attempts exceed the configured threshold in the applied credential policy.</td>
</tr>
<tr>
<td>Logon Attempts</td>
<td></td>
</tr>
</tbody>
</table>

**Associate devices to application users**

**Before You Begin**

To assign devices to an application user, you must access the Application User Configuration window for that user. Use the Finding an Application User window (User Management > Application User) to find an application user. When the Application User Configuration window displays, perform the following procedure to assign devices.

**Procedure**

**Step 1**
In the Available Devices list box, choose a device that you want to associate with the application user and click the Down arrow below the list box. The selected device moves to the applicationuser.controlledDevices list box.

**Step 2**
To limit the list of available devices, click the Find more Phones, Find more Route Points, or Find more Pilot Points button:
a) If you click the Find more Phones button, the Find and List Phones window displays. Perform a search to find the phones to associate with this application user.
b) If you click the Find more Route Points button, the Find and List CTI Route Points window displays. Perform a search to find the CTI route points to associate with this application user.
c) If you click the Find more Pilot Points button, the Find and List Pilot Points window displays. Perform a search to find the pilot points to associate with this application user.

**Step 3** Repeat the preceding steps for each device that you want to assign to the application user.

**Step 4** When you complete the assignment, click Save to assign the devices to the application user.

**Related Topics**

Application user setup, on page 759
End user setup

This chapter provides information about managing end user directory information.

- About end user setup, page 771
- End user deletion, page 772
- End user settings, page 773
- Create Cisco Unity Connection voice mailbox, page 779
- Change end user password, page 781
- Change end user PIN, page 781
- Manage end user credential information, page 782
- Credential settings and fields, page 782
- Set up end user information, page 784
- Associate devices to end user, page 785
- Associate Cisco Extension Mobility profile to Cisco Unified IP Phone, page 786

About end user setup

In Cisco Unified Communications Manager (Unified CM) Administration, use the User Management > End User menu path to configure end users.

The End User Configuration window in Unified CM Administration allows the administrator to add, search, display, and maintain information about Unified CM end users. End users can control phones after you associate a phone in the End User Configuration window. You can also enable end users for IM and Presence.

End user setup tips

Consult the following information before you begin to configure end users:

- To verify whether the Enable Synchronizing from LDAP Server check box is checked, choose System > LDAP > LDAP System. If the check box is checked, LDAP synchronization is enabled; if not, LDAP synchronization is disabled.
• If you enable LDAP synchronization in Unified CM Administration, you cannot change some existing user information, including user IDs, for LDAP synchronized users in the End User Configuration windows. Instead, you must use the corporate LDAP directory to update some user information for those users. For local users, all the user information remains editable.

• If you configure your system to authenticate users against the LDAP directory, you cannot configure or change end user passwords for LDAP synchronized users in Unified CM Administration. You configure and change end user passwords for those users in the corporate LDAP directory. For local users, you configure and change the end user passwords in Unified CM Administration.

• You can import Cisco Unity Connection users in Cisco Unity Connection, as described in the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. Or, if you want to do so, you can configure a Unified CM Administration end user as a Cisco Unity Connection user by using the Create a Cisco Unity User option in the End User Configuration window. You can then configure any additional settings in Cisco Unity Connection Administration.

Note

Before you can create a Cisco Unity Connection mailbox for the end user, you must configure the end user with a phone device association and a primary extension, and the integration between Unified CM and Cisco Unity Connection must be complete. For more information, see the Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection or the Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection.

Next Steps to configure an end user

You can associate devices to this end user and manage the end user credentials.

You can create a Cisco Unity Connection Voice Mailbox for this user in Unified CM Administration.

You can specify this cluster as the home cluster for the end user.

You can configure this end user for IM and Presence service.

You can associate a service profile to this end user.

You can associate users to their line appearances for presence.

Related Topics

  Manage application user credential information, on page 767
  Create Cisco Unity Connection voice mailbox, on page 779
  Associate devices to end user, on page 785

End user deletion

Before you delete an end user, determine whether you must remove the devices or profiles that are associated with the end user.

You can view the devices and profiles that are assigned to the end user from the Device Associations, Extension Mobility, Directory Number Associations, CAPF Information, and Permissions Information areas of the End User Configuration window. You can also choose Dependency Records from the Related Links drop-down list box in the End User 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.
Next steps

If this user is configured in Cisco Unity Connection, the user association to Cisco Unified Communications Manager (Unified CM) is broken when you delete the user in Unified CM Administration. You can delete the orphaned user in Cisco Unity Connection Administration. See the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection. Deleting the user deletes all messages in the user voice mailbox.

Related Topics

Access dependency records, on page 874

End user settings

The following table describes the end user settings.

Table 116: End user settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Information</td>
<td></td>
</tr>
<tr>
<td>User Status</td>
<td>This field indicates whether the user is a local user or LDAP synchronized.</td>
</tr>
<tr>
<td>User ID</td>
<td>Enter the unique end user identification name. You can enter any character, including alphanumeric and special characters. No character restrictions exist for this field. You can modify the user ID only for local users. For LDAP synchronized users, you can view the user ID, but you cannot modify it.</td>
</tr>
<tr>
<td>Password/Edit Credential</td>
<td>This field does not display for LDAP synchronized users if LDAP Authentication is enabled. Enter alphanumeric or special characters for the end user password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters). The Edit Credential button displays after this user is added to the database. Click the Edit Credential button to manage credential information for this user.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>This field does not display for LDAP Synchronized users if LDAP Authentication is enabled. Enter the end user password again.</td>
</tr>
<tr>
<td>PIN/Edit Credential</td>
<td>Enter numeric characters for the end user PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters). The Edit Credential button appears after you add this user to the database. Click the Edit Credential button to manage credential information for this user.</td>
</tr>
<tr>
<td>Confirm PIN</td>
<td>Enter the PIN again.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the end user last name.</td>
</tr>
<tr>
<td>Middle Name</td>
<td>Enter the end user middle name.</td>
</tr>
<tr>
<td>First Name</td>
<td>Enter the end user first name.</td>
</tr>
<tr>
<td>Directory URI</td>
<td>Enter the directory URI that you want to associate to this end user. A directory URI looks like an email address and follows the user@host format. For information about valid formats for directory URIs, see Directory URI formats in the “Intercluster Directory URI” chapter of the <em>Cisco Unified Communications Manager Administrative Guide</em>. Note: If you enter a directory URI and also enter a directory number in the Primary Extension field, this directory URI automatically becomes the primary directory URI that is associated to that directory number.</td>
</tr>
<tr>
<td>Mail ID</td>
<td>Enter the end user e-mail address.</td>
</tr>
<tr>
<td>Manager User ID</td>
<td>Enter the user ID of the end user manager ID. The manager user ID that you enter does not have to exist in the same cluster as the end user; therefore, Unified CM does not require that you enter a user ID that already exists in the database.</td>
</tr>
<tr>
<td>Department</td>
<td>Enter the end user department information (for example, the department number or name).</td>
</tr>
<tr>
<td>User Locale</td>
<td>From the drop-down list box, choose the locale that is associated with the end user. The user locale identifies a set of detailed information to support end users, including language and font. Unified CM uses this locale for extension mobility and the Cisco Unified CM User Options. For Cisco Extension Mobility login, the locale that is specified takes precedence over the device and device profile settings. For Cisco Extension Mobility logout, Unified CM uses the end user locale that the default device profile specifies. Note: If you do not choose an end user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.</td>
</tr>
<tr>
<td>Associated PC</td>
<td>This required field applies for Cisco IP Softphone users.</td>
</tr>
<tr>
<td>Digest Credentials</td>
<td>Enter a string of alphanumeric characters. Unified CM uses the digest credentials that you specify here to validate the credentials that the phone offers during digest authentication. The digest credentials that you enter in this field get associated with the phone when you choose a digest user in the Phone Configuration window. Note: For more information about digest authentication, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Digest Credentials</td>
<td>To confirm that you entered the digest credentials correctly, re-enter the credentials in this field.</td>
</tr>
</tbody>
</table>

#### Convert User Account

| Convert LDAP Synchronized User to Local User | This check box appears for LDAP synchronized end users. Check this check box then save changes to convert an LDAP synchronized user to a local user. |

#### Service Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Cluster</td>
<td>Check this check box if the end user is homed to this cluster. The end user should only be homed to one cluster within the enterprise. <strong>Note</strong> IM and Presence does not function properly if an end user is assigned to more than one home cluster.</td>
</tr>
<tr>
<td>Enable User for IM and Presence</td>
<td>Check this check box to enable the end user (on the home cluster) for IM and Presence. Configure IM and Presence in the associated service profile. <strong>Note</strong> You must install a Unified CM IM and Presence node along with this Unified CM cluster. Use the <strong>User Management &gt; User Settings &gt; UC Services</strong> menu to configure the IM and Presence service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC Service Profile</td>
<td>Choose a UC service profile from the drop-down list box. To view the settings for each UC service profile, click the More Details link.</td>
</tr>
</tbody>
</table>

#### Device Associations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled Devices</td>
<td>After you associate the device, this field displays the description information (for example, the MAC address) that the end user controls. Adding a device to the list of controlled devices for the end user does not move the device from “Unassigned Devices” to “Users” in the License Usage Report. You must assign a user ID to the device. <strong>Note</strong> To associate a line appearance to this end user for presence, select the Line Appearance Association from Presence button. Doing so enables the on-the-phone status information to IM and Presence clients when this line appearance is off-hook. The Line Appearance choices presented depend on the lines associated with the controlled devices. <strong>Note</strong> If you want additional line appearance associations, or multiple user associations for a single line appearance, choose <strong>Call Routing &gt; Directory Number</strong> to see the Directory Number window.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Profiles</td>
<td>This drop-down list box displays the device profiles that are available for association with this end user.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CTI Controlled Profiles</td>
<td>This drop-down list box displays the CTI-controlled profiles that are available for association with an end user who is configured for CTI.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Extension Mobility is not supported for third-party AS-SIP.</td>
</tr>
<tr>
<td>Available Profiles</td>
<td>This list box displays the extension mobility profiles that are available for association with this end user.</td>
</tr>
<tr>
<td></td>
<td>To search for an extension mobility profile, click Find. Use the Find and List Device Profiles window that appears to search for the extension mobility profile that you want.</td>
</tr>
<tr>
<td></td>
<td>To associate an extension mobility profile with this end user, select the profile and click the Down arrow below this drop-down list box.</td>
</tr>
<tr>
<td>Controlled Profiles</td>
<td>This field displays a list of controlled device profiles that are associated with an end user who is configured for Cisco Extension Mobility.</td>
</tr>
<tr>
<td>Default Profile</td>
<td>From the drop-down list box, choose a default extension mobility profile for this end user.</td>
</tr>
<tr>
<td>BLF Presence Group</td>
<td>Use this field to configure the BLF Presence feature.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, choose a BLF presence group for the end user. The selected group specifies the destinations that the end user can monitor.</td>
</tr>
<tr>
<td></td>
<td>The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF Presence Groups that are configured in Unified CM Administration also appear in the drop-down list box.</td>
</tr>
<tr>
<td></td>
<td>BLF Presence Group authorization works with BLF Presence Groups to allow or block presence requests between groups. See the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td>SUBSCRIBE Calling Search Space</td>
<td>Supported with the BLF Presence feature, the SUBSCRIBE calling search space determines how Unified CM routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user.</td>
</tr>
<tr>
<td></td>
<td>From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Unified CM Administration appear in the SUBSCRIBE Calling Search Space drop-down list box.</td>
</tr>
<tr>
<td></td>
<td>If you do not select a different calling search space for the end user from the drop-down list box, the SUBSCRIBE calling search space defaults to None.</td>
</tr>
<tr>
<td></td>
<td>To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Allow Control of Device from CTI | If this check box is checked, when the user logs in to a device, the AllowCTIControlFlag device property becomes active, which allows control of the device from CTI applications. Until the user logs in to a device, this setting has no effect. **Note** The Allow Control of Device from CTI setting in the end user configuration overrides the AllowCTIControlFlag device property of the device to which the user logs in.

Enable Extension Mobility Cross Cluster | Check this box to enable this end user to use the Cisco Extension Mobility Cross Cluster feature.

| Note | For more information about the Cisco Extension Mobility Cross Cluster feature, see the *Cisco Unified Communications Manager Features and Services Guide*. |

Directory Number Associations | 
Primary Extension | This field represents the primary directory number for the end user. End users can have multiple lines on their phones.

When you associate devices to the end user, directory numbers that are configured on the associated device become available in the drop-down list box for Primary Extension. From the drop-down list box, choose a primary extension for this end user.

If the system is integrated with Cisco Unity Connection, the Create Cisco Unity User link displays in the Related Links menu.

IPCC Extension | From the drop-down list box, choose an IPCC extension for this end user. **Note** This field appears only if the IPCC Express Installed enterprise parameter is set to True.

Mobility Information | 
Enable Mobility | Check this check box to activate Mobile Connect, which allows the user to manage calls by using a single phone number and to pick up in-progress calls on the desktop phone and cellular phone.

Checking this check box, which triggers licensing to consume device license units for Mobile Connect, works in conjunction with the Primary User Device drop-down list box.

If you check the Enable Mobility check box and fail to choose an adjunct device from the Primary User Device drop-down list box, four device license units (DLUs) are consumed, as indicated in the Mobility Enabled End Users row in the License Unit Calculator window.

If you enable Cisco Unified Mobility and later choose an adjunct device from the Primary User Device drop-down list box, the system credits you with two DLUs, as indicated in the Mobility Enabled End Users row in the License Unit Calculator window.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Primary User Device         | The Primary User Device drop-down list box, which works in conjunction with the Enable Mobility check box, controls the number of device license units that are consumed for adjunct devices for Mobile Connect. After you check the Enable Mobility check box, choose an adjunct device that you want to assign to the user specifically for Cisco Unified Mobility. For example, choose a device, such as a desktop phone, that the user uses in addition to the cell phone for Cisco Unified Mobility. Before you choose an adjunct device, consider the following information:  
  • Only devices that consume two or more DLUs appear in the drop-down list box.  
  • For Cisco Unified Mobility, you cannot assign the same device to multiple users, so only the devices that you can assign display in the drop-down list box.  
  • If you check the Enable Mobility check box and choose a device from the drop-down list box, two DLUs get consumed, as indicated in the Mobility Enabled End Users (Adjunct) row in the Licensing Unit Calculator window.  
  • If you delete the device from Unified CM Administration or remove the assignment after you enable Mobile Connect, two DLUs are 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. |
| Enable Mobile Voice Access  | Check this check box to allow the user to access the Mobile Voice Access integrated voice response (IVR) system to initiate Mobile Connect calls and activate or deactivate Mobile Connect capabilities.                             |
| Maximum Wait Time for Desk Pickup | Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to desktop phone.                                                                                   |
| Remote Destination Limit    | Enter the maximum number of phones to which the user is permitted to transfer calls from the desktop phone.                                                                                                      |
| Remote Destination Profiles | This field lists the remote destination profiles that were created for this user. To view the details of a particular remote destination profile, choose a remote destination profile in the list and click the View Details link. |
| Mutilevel Precedence and Preemption Authorization |                                                                                                                                                                                                            |
| MLPP User Identification Number | This pane displays the Instance ID from the CAPF Profile that you configured for this user. To view or update the profile, double-click the Instance ID or click the Instance ID to highlight it; then, click View Details. The End User CAPF Profile Configuration window displays with the current settings.  
  **Note** The MLPP User Identification number must comprise 6 - 20 numeric characters.  
  For information on how to configure the End User CAPF Profile, see the *Cisco Unified Communications Manager Security Guide*. |
Create Cisco Unity Connection voice mailbox

The Create Cisco Unity User link on the End User Configuration window allows you to create individual Cisco Unity Connection voice mailboxes in Cisco Unified Communications Manager (Unified CM) Administration.

Before You Begin

- You must configure Unified CM for voice messaging.
- You must configure the Cisco Unity Connection server to use the integrated mailbox feature. See the “Creating Multiple User Accounts from Unified CM Users” chapter of the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Password</td>
<td>Enter the MLPP password.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The MLPP Password must comprise 4 - 20 numeric characters.</td>
</tr>
<tr>
<td>Confirm MLPP Password</td>
<td>Confirm the MLPP password.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To confirm that you entered the MLPP Password correctly, re-enter the password in this field.</td>
</tr>
<tr>
<td>MLPP Precedence Authorization Level</td>
<td>Set the MLPP Precedence Authorization Level.</td>
</tr>
<tr>
<td></td>
<td>The following precedence levels indicate the priority level that is associated with a call:</td>
</tr>
<tr>
<td></td>
<td>• 0: Flash Override (highest)</td>
</tr>
<tr>
<td></td>
<td>• 1: Flash</td>
</tr>
<tr>
<td></td>
<td>• 2: Immediate</td>
</tr>
<tr>
<td></td>
<td>• 3: Priority</td>
</tr>
<tr>
<td></td>
<td>• 4: Routine (lowest)</td>
</tr>
<tr>
<td></td>
<td>You can set the Precedence Authorization Level to any standard precedence level from Routine to Executive Override.</td>
</tr>
<tr>
<td></td>
<td>Calls of equal or lower precedence are authorized to be originated by the user.</td>
</tr>
</tbody>
</table>

Related Topics

- Calling search space setup, on page 247
- End user setup, on page 771
- Associate devices to end user, on page 785
- Role setup, on page 787
- Access control group setup, on page 791
• For Cisco Unity Connection integration, create an AXL connection via Cisco Unity Connection, as described in the "Managing the Phone System Integrations" chapter in the System Administration Guide for Cisco Unity Connection.

• Ensure that you define an appropriate template and Class of Service (COS) for any voice-messaging users that you plan to add in Unified CM Administration. For Cisco Unity Connection users, see the applicable User Moves, Adds, and Changes Guide for Cisco Unity Connection.

• You must associate a device and a Primary Extension Number to the end user before the Create Cisco Unity User link displays. The link appears in the Related Links menu.

• You can use the import feature that is available in Cisco Unity Connection instead of performing the procedure that is described in this section. For information about how to use the import feature, see the “Creating Multiple User Accounts from Unified CM Users” chapter of the User Moves, Adds, and Changes Guide for Cisco Unity Connection.

Note

The Directory Number Configuration window also displays the “Create Cisco Unity User” link in the Related Links drop-down list box.

Procedure

Step 1 Use the User Management > End User menu option to find the end user.

Step 2 Verify that a primary extension number is associated with this user.

Note You must define a primary extension; otherwise, the Create Cisco Unity User link does not appear in the Related Links drop-down list box.

Step 3 From the Related Links drop-down list box, choose the Create Cisco Unity User link, and then click Go. The Add Cisco Unity User dialog box appears.

Step 4 From the Application Server drop-down list box, choose the Cisco Unity Connection server on which you want to create a Cisco Unity Connection user, and then click Next.

Step 5 From the Subscriber Template drop-down list box, choose the subscriber template that you want to use.

Step 6 Click Save.

The mailbox is created. The link in the Related Links drop-down list box changes to Edit Cisco Unity User in the End User Configuration window. In Cisco Unity Connection Administration, you can now view the user that you created.

Note After you integrate the Cisco Unity Connection user with the Unified CM end user, you cannot edit fields in Cisco Unity Connection Administration such as Alias (User ID in Unified CM Administration), First Name, Last Name, and Extension (Primary Extension in Unified CM Administration). You can only update these fields in Unified CM Administration.

Related Topics

End user setup, on page 771
Change end user password

Use the following procedure to change the password for an end user in Cisco Unified Communications Manager Administration.

---

**Note**

You cannot change an end user password when LDAP authentication is enabled.

---

**Procedure**

**Step 1**

Use the **User Management > End User** menu option to find the end user. The End User Configuration window displays the configuration information.

**Step 2**

In the Password field, double-click the existing password, which is encrypted, and enter the new password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

**Step 3**

In the Confirm Password field, double-click the existing, encrypted password and enter the new password again.

**Step 4**

Click Save.

---

**Related Topics**

- End user setup, on page 771

Change end user PIN

Use the following procedure to change the personal identification number (PIN) for an end user.

---

**Procedure**

**Step 1**

Use the **User Management > End User** menu option to find the end user. The End User Configuration window displays the configuration information.

**Step 2**

In the PIN field, double-click the existing PIN, which is encrypted, and enter the new PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

**Step 3**

In the Confirm PIN field, double-click the existing, encrypted PIN and enter the new PIN again.

**Step 4**

Click Save.

---

**Related Topics**

- End user setup, on page 771
Manage end user credential information

Use the following procedure to change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an end user. You can edit user credentials only after the user exists in the database.

In the user Credential Configuration window, you cannot save settings that conflict with the assigned credential policy.

In the user Credential Configuration window, you cannot change settings that conflict with other settings in the user Credential Configuration window. For example, if the User Cannot Change check box is checked, you cannot check the User Must Change at Next Login check box.

The credential configuration window reports approximate event times; the system updates the form at the next authentication query or event.

Before You Begin
Create the end user in the database.

Procedure

Step 1 Use the User Management > End User menu option to find the end user. The End User Configuration window displays the configuration information.

Step 2 To change or view password information, click the Edit Credential button next to the Password field. To change or view PIN information, click the Edit Credential button next to the PIN field.

Step 3 Enter the appropriate settings as described in Table 117: Application user and end user credential settings and fields, on page 782.

Step 4 If you have changed any settings, click Save.

Related Topics
End user setup, on page 771
About end user setup, on page 771

Credential settings and fields

The following table describes the credential settings for end users and application users. These settings do not apply to application user or end user digest credentials.

Table 117: Application user and end user credential settings and fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked By Administrator</td>
<td>Check this check box to lock this account and block access for this user.</td>
</tr>
<tr>
<td></td>
<td>Uncheck this check box to unlock the account and allow access for this user.</td>
</tr>
</tbody>
</table>
### Field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Cannot Change</td>
<td>Check this check box to block this user from changing this credential. Use this option for group accounts. You cannot check this check box when User Must Change at Next Login check box is checked.</td>
</tr>
<tr>
<td>User Must Change at Next Login</td>
<td>Check this check box to require the user to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when User Cannot Change check box is checked.</td>
</tr>
<tr>
<td>Does Not Expire</td>
<td>Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If this check box is checked, the user can still change this credential at any time. When this check box is unchecked, the expiration setting in the associated credential policy applies.</td>
</tr>
<tr>
<td>Reset Hack Count</td>
<td>Check this check box to reset the hack count for this user and clear the Time Locked Due to Failed Login Attempts field. After the counter resets, the user can try logging in again. The hack count increments whenever an authentication fails for an incorrect credential. If the policy specifies No Limit for Failed Logons, the hack count always equals 0.</td>
</tr>
<tr>
<td>Authentication Rule</td>
<td>Select the credential policy to apply to this user credential.</td>
</tr>
<tr>
<td>Time Last Changed</td>
<td>This field displays the date and time of the most recent change for this user credential.</td>
</tr>
<tr>
<td>Failed Logon Attempts</td>
<td>This field displays the number of failed login attempts since the last successful login, since the administrator reset the hack count for this user credential, or since the reset failed login attempts time has expired.</td>
</tr>
<tr>
<td>Time of Last Failed Logon Attempt</td>
<td>This field displays the date and time for the most recent failed login attempt for this user credential.</td>
</tr>
<tr>
<td>Time Locked by Administrator</td>
<td>This field displays the date and time that the administrator locked this user account.</td>
</tr>
<tr>
<td>Time Locked Due to Failed Logon Attempts</td>
<td>This field displays the date and time that the system last locked this user account due to failed login attempts. The associated credential policy defines lockouts due to failed login attempts.</td>
</tr>
</tbody>
</table>
Set up end user information

After you add a new end user, you can configure additional information that is related to the end user. This information allows each end user to personalize phone features, Manager Configuration, Assistant Configuration, Cisco Extension Mobility, Cisco Unified Communications Manager Auto-Attendant, and Cisco IP Softphone capability.

Before You Begin
Make sure that the end user is in the database.

Procedure

Step 1
Use the User Management > End User menu option to find the end user whose application profiles you want to configure.

The End User Configuration window appears with information about the chosen end user.

Step 2
Click the user ID.

Step 3
To configure a manager for Cisco Unified Communications Manager Assistant for this end user, from the Related Links drop-down list box, choose Manager Configuration, and then click Go.

The Manager Configuration window appears for this end user. For more information about configuring Cisco Unified Communications Manager Assistant, see topics related to Cisco Unified Communications Manager Assistant with proxy line support and shared line support in the Cisco Unified Communications Manager Features and Services Guide.

After you configure the manager information for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the Manager Configuration window, choose Back to User Configuration, and then click Go.

Step 4
To configure an assistant for Cisco Unified Communications Manager Assistant for this end user, from the Related Links drop-down list box, choose Assistant Configuration, and then click Go.

The Assistant Configuration window appears for this end user. For more information about configuring Cisco Unified Communications Manager Assistant, see topics related to Cisco Unified Communications Manager Assistant with proxy line support and shared line support in the Cisco Unified Communications Manager Features and Services Guide.

After you configure the assistant information for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the Assistant Configuration window, choose Back to User Configuration and click Go.

Step 5
To show the user privilege report for this end user, from the Related Links drop-down list box, choose User Privilege Report, and then click Go.

The User Privilege window appears for this end user.

After you display the user privilege report for this end user, you can return to the End User Configuration window for this end user. From the Related Links drop-down list box in the User Privilege window, choose Back to User, and then click Go.
You can associate devices over which end users have control. End users can control some devices, such as phones. Applications that are identified as users can control other devices, such as CTI ports. When end users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding.

For devices that are not CTI-controllable, such as H.323 devices, an asterisk (*) appears next to the device icon in the list of available devices. All device association behavior remains identical regardless of the type of device for which the feature is configured.

**Before You Begin**

To associate devices with an end user, you must access the End User Configuration window for that user. Use the **User Management > End User** menu option to find the end user. When the End User Configuration window appears, perform the following procedure to assign devices.

Do not attempt to associate devices to a new end user before you finish adding the new end user. Be sure to click Save on the End User Configuration window before you add device associations for a new end user.

**Procedure**

**Step 1**

In the Device Associations pane, click **Device Association**.

The User Device Association window appears.

Because you may have several devices in your network, Cisco Unified Communications Manager (Unified CM) lets you locate specific devices on the basis of specific criteria. Use the following steps to locate devices.

**Note**

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

**Step 2**

To find all records in the database, ensure the dialog box is empty; go to **Step 3**, on page 785.

a) From the first drop-down list box, select a search parameter.

b) From the second drop-down list box, select a search pattern.

c) 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 or matching records appear. You can change the number of items that appears in each window by choosing a different value from the Rows per Page drop-down list box.

Associating a Device
Step 4  From the Device association for (this particular user) pane, choose the devices that you want to associate with this end user by checking the box to the left of the device names. Use the buttons at the bottom of the window to select and deselect devices to associate with the end user.

Note  The buttons function to select and deselect only the devices that were found as a result of any search for devices that you performed in the preceding steps.

Tip  Check the Show the devices already associated with user check box to display the devices that are already associated with this end user.

Use the buttons to perform the following functions:

a)  **Select All**: Click this button to select all devices that appear in this window.

b)  **Clear All**—Click this button to uncheck the check boxes next to all devices that appear in this window.

c)  **Select All in Search**—Click this button to select all devices that match the search criteria that you specified in the Search Options portion of the window. The button performs the search anew and selects all the matching devices.

d)  **Clear All in Search**—Click this button to deselect all devices that match the search criteria that you specified in the Search Options portion of the window. The button performs the search anew and deselects all the matching devices.

e)  **Save Selected/Changes**—Click this button to associate the devices that you selected with this end user.

f)  **Remove All Associated Devices**—Click this button to disassociate all devices that are already associated with this end user. After you click this button, a dialog box asks you to confirm that you want to remove all device associations from this end user. To confirm, click OK.

Step 5  Repeat the preceding steps for each device that you want to assign to the end user.

Step 6  To complete the association, click **Save Selected/Changes**.

Step 7  From Related Links drop-down list box, choose Back to User, and then click **Go**.

The End User Configuration window appears, and the associated devices that you chose appear in the Controlled Devices pane.

---

**Related Topics**

End user setup, on page 771

---

**Associate Cisco Extension Mobility profile to Cisco Unified IP Phone**

Use Cisco Extension Mobility to configure a Cisco Unified IP Phone to temporarily display as the phone of an end user. The end user can sign in to a phone, and the Extension Mobility profile (including line and speed-dial numbers) for the end user resides on the phone. This feature applies primarily in environments where end users are not permanently assigned to physical phones.

- To associate an Extension Mobility profile to an end user, you must access the End User Configuration window for that end user. Use the **User Management > End User** menu option to find the end user. To configure and associate Cisco Extension Mobility for end users, see the *Cisco Unified Communications Manager Features and Services Guide*.

**Related Topics**

End user setup, on page 771
Role setup

This chapter provides information to configure roles.

- Role setup, page 787
- Role deletions, page 788
- Role settings, page 788

Role setup

In Cisco Unified Communications Manager Administration, use the User Management > Role menu path to configure roles.

Roles allow Cisco Unified Communications Manager administrators who have full administration privilege (access) to configure end users and application users with different levels of privilege. Administrators with full administration privilege configure roles and user groups. In general, full-access administration users configure the privilege of other administration users and end users to Cisco Unified Communications Manager Administration and to other applications.

Different levels of privilege exist for each application. For example, for Cisco Unified Communications Manager Administration, two levels of privilege exist: read privilege and update privilege. These privilege levels differ as follows:

- Users with update privilege can view and modify the Cisco Unified Communications Manager Administration windows to which the user group of the user has update privilege.
- A user with read privilege can view the Cisco Unified Communications Manager Administration windows that belong to the roles to which the user group of the user has read privilege. A user with read privilege for a window cannot, however, make any changes on those administration windows to which the user has only read privilege. For a user with read privilege, the Cisco Unified Communications Manager Administration application does not display any update buttons or icons.

Roles comprise groups of resources for an application. If you want to do so, you can create custom roles that comprise custom groupings of resources for an application. At installation, default standard roles are created for various administrative functions. For example, to configure Audit Log Administration, choose the Standard Audit Log Administration role. When the Role Configuration window displays, check the Read or Update check box for the resource you want to configure and click Save.
Certain standard roles have no associated application nor resource. These roles provide login authentication for various applications.

**Tip**

Example add or copy roles

To configure Audit Log Administration, choose the Standard Audit Log Administration role. When the Role Configuration window displays, click the Read or Update check box for the resource that you want to configure and click Save.

**Note**

Copying a role also copies the privileges that are associated with that role.

If you are adding a new role, choose an application from the Application drop-down list box and click Next. In the Role Configuration window that displays, enter the appropriate settings as described in Table 118: Role settings, on page 788.

**Role deletions**

You cannot delete a standard role.

**Role settings**

The following table describes the role settings.

*Table 118: Role settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Information</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>From the drop-down list box, choose the application with which this role associates.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name for the role. Names can comprise up to 128 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the role. Descriptions can have up to 128 characters.</td>
</tr>
<tr>
<td>Resource Access Information</td>
<td></td>
</tr>
</tbody>
</table>
In the Resource Access Information pane, click the checkbox(es) next to the resource(s) that you want this role to include.

**Note** In some applications, only one checkbox applies for each resource. In the Cisco Unified Communications Manager Administration application, a read checkbox and an update checkbox apply to each resource.

Click this button to grant privileges for all resources that display on this page for this role.

**Note** If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access of the resources that are listed on those pages.

Click this button to remove privileges for all resources that display on this page for this role.

**Note** If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access of the resources that are listed on those pages.

### Related Topics

Role setup, on page 787
Access control group setup

This chapter provides information to configure access control groups, assign users to access control groups, and view the roles, access control groups, and permissions of a user.

- About access control group setup, page 791
- Find access control group, page 792
- Set up access control group, page 793
- Delete access control group, page 794
- Add users to access control groups, page 794
- Delete users from access control groups, page 796
- Assign roles to access control group, page 796
- View user roles, access control groups, and permissions, page 797

About access control group setup

The role and access control group menu options in the Cisco Unified Communications Manager (Unified CM) Administration User Management menu allow users with full access to configure different levels of access for Unified CM administrators. Users with full access configure roles, access control groups, and access privileges for roles. In general, full-access users configure the access of other users to Unified CM Administration.

Access control groups comprise lists of application users and end users. A user may belong to multiple access control groups. After you add an access control group, you then add users to an access control group. After these steps, you can assign roles to an access control group. If a user belongs to multiple access control groups, the MLA permission enterprise parameter determines the effective privilege of the user.

Reduced permissions for Access Control Groups

Users can belong to multiple access control groups. When adding a new access control group to existing users, an unexpected reduction in the current level of privileges for some pre-existing access control groups may be experienced if the new access control group has the "Effective Access Privileges for Overlapping User Groups and Roles" Enterprise parameter set to minimum.
Access privilege reduction can occur inadvertently, for example, during an upgrade of Cisco Unified Communications Manager Administration. If the upgrade version supports the Standard RealTimeAndTrace Collection user group, which has the "Effective Access Privileges for Overlapping User Groups and Roles" Enterprise parameter set to minimum, all users are automatically added to that user group during the upgrade. To resolve the permissions issue in this example, you can remove users from the Standard RealTimeAndTrace Collection user group.

Find access control group

Because you might have several access control groups in your network, Cisco Unified Communications Manager (Unified CM) lets you locate specific access control groups on the basis of specific criteria. Use the following procedure to locate access control group.

Note During your work in a browser session, Unified CM Administration retains your access control group search preferences. If you navigate to other menu items and return to this menu item, Unified CM Administration retains your access control group search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose User Management > User Settings > Access Control Group.
The Find and List Access Control Groups window appears. 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.
a) From the drop-down list box, select a search pattern.
b) 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 appear. You can change the number of items that appear 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 then clicking Delete Selected. You can delete all configurable records for this selection by clicking Select All, and then clicking Delete Selected.

Note You cannot delete the standard access control groups.

Step 4 From the list of records that appear, 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.
Set up access control group

This section describes how to add, copy, and update an access control group to and in the Cisco Unified Communications Manager Administration.

The following example provides more detail about configuring an access control group.

To allow a user to change Audit Log settings, choose Standard Audit Users, and then click Add End Users to Group. When the Find and List Users window appears, choose the user that you want to add to the group and click Add Selected.

Procedure

Step 1  Choose User Management > User Settings > Access Control Group. The Find and List Access Control Group window appears.

Step 2  Perform one of the following tasks:
   a) To copy an existing access control group, locate the appropriate access control group, and then click Copy next to the access control group that you want to copy. In the popup window that appears, enter a name for the new access control group, and then click OK. Continue with Step 3, on page 793.
   b) To add a new access control group, click Add New. Enter a name for the new access control group, and then click OK. Continue with Step 3, on page 793.
      Note The access control group name can contain up to 50 alphanumeric characters and can contain any combination of spaces, periods (.), hyphens (-), and underscore characters (_). Ensure that the access control group name is unique.
   c) To update an existing access control group, locate the appropriate access control group. Click the name of the access control group that you want to update. The access control group that you chose appears. Update the appropriate settings. Continue with Step 3, on page 793.
      Note You cannot delete a standard access control group, but you can update the user membership for a standard access control group.

Step 3  Click Save.

Step 4  Add users to this access control group.

Step 5  Assign roles to the access control group.

Related Topics

   Access control group setup, on page 791
   Find access control group, on page 792
   Add users to access control groups, on page 794
   Assign roles to access control group, on page 796
Delete access control group

This section describes how to delete an access control group from Unified CM Administration. Use the following procedure to delete an access control group entirely.

Before You Begin

When you delete an access control group, Cisco Unified Communications Manager (Unified CM) removes all access control group data from the database. To find out which roles are using the access control group, in the Access Control Group Configuration window, choose Dependency Records from the Related Links drop-down list box, and then click Go. If dependency records are not enabled for the system, the Dependency Records Summary window displays a message.

Procedure

Step 1 Choose User Management > User Settings > Access Control Group. The Find and List Access Control Groups window appears.

Step 2 Find the access control group that you want to delete.

Step 3 Click the name of the access control group that you want to delete. The access control group that you chose appears. The list shows the users in this access control group in alphabetical order.

Step 4 If you want to delete the access control group entirely, click Delete. A dialog box appears to warn you that you cannot undo the deletion of access control groups.

Step 5 To delete the access control group, click OK or to cancel the action, click Cancel. If you click OK, Unified CM removes the access control group from the database.

Related Topics

Access control group setup, on page 791
Find access control group, on page 792
Delete users from access control groups, on page 796
Access dependency records, on page 874

Add users to access control groups

This section describes how to add end users and application users to an access control group in Cisco Unified Communications Manager (Unified CM) Administration.

Procedure

Step 1 Choose User Management > User Settings > Access Control Group. The Find and List Access Control Groups window appears.
Add users to access control groups

Step 2  Find the access control group to which you want to add users.

Step 3  Click the name of the access control group that you want to update.
        The access control group that you chose appears. The Users list shows the users that currently belong to the access control group.

Step 4  To add end users, click Add End Users to Group. To add application users, skip to step 8.
        The Find and List Users window appears.

Step 5  Use the Find User drop-down list boxes to find the end users that you want to add, and then click Find.
        Note: You can perform the search for users in a variety of ways. You can enter the first name, middle name, last name, user ID, or department of a user. Alternatively, you can leave the field blank, which results in display of all users.
        A list of end users that matches your search criteria appears.
        Note: The list of search results does not display end users that already belong to the access control group.

Step 6  In the list of search results, check the check box next to the users that you want to add to this access control group. If the list comprises multiple pages, use the links at the bottom to see more results.

Step 7  Click Add Selected.
        The Access Control Group Configuration window reappears with the users that you added listed in the Users pane.
        Note: After you add a user, you can view the roles by clicking the i icon in the Permission column for that user.

Step 8  To add application users, click Add App Users to Group.
        The Find and List Application Users window appears.

Step 9  Use the Find Application User drop-down list boxes to find the application users that you want to add and click Find.
        Note: You can perform the search for application users by searching for user ID. Alternatively, you can leave the field blank, which results in display of all application users.
        A list of application users that matches your search criteria displays.

Step 10 In the list of search results, check the check box next to the application users that you want to add to this access control group. If the list comprises multiple pages, use the links at the bottom to see more results.
        Note: The list of search results does not display application users that already belong to the user group.

Step 11 Click Add Selected.
        The Access Control Group Configuration window reappears with the application users that you added listed in the Users pane.
        Note: After you add an application user, you can view the roles by clicking the i icon in the Permission column for that user.

Step 12 To save your changes to this access control group, click Save.

Related Topics

Access control group setup, on page 791
Find access control group, on page 792
Delete users from access control groups

This section describes how to delete users from an access control group in Cisco Unified Communications Manager (Unified CM) Administration.

Procedure

Step 1 Choose User Management > User Management > Access Control Group. The Find and List Access Control Groups window appears.

Step 2 Find the access control group from which you want to delete users.

Step 3 Click the name of the access control group that you want to update. The access control group that you chose appears. The Users list shows the users that currently belong to the access control group.

Step 4 Check the check boxes next to the names of the users that you want to delete from this access control group.

Step 5 Click Delete Selected. A confirmation message asks you to confirm the deletion.

Step 6 To delete the selected access control group members, click OK or Cancel to exit this window. The Access Control Group Configuration reappears with the deleted users removed from the Users in Group pane.

Related Topics

Access control group setup, on page 791
Find access control group, on page 792

Assign roles to access control group

Users with full access can assign roles to access control groups. An access control group that has assigned roles has access to the resources that the role comprises.

This section describes assigning roles to an access group in Cisco Unified Communications Manager (Unified CM) Administration.

Note

When an administrator assigns roles to an access control group, the administrator should assign the Standard Unified CM Admin Users role to the access control group. This role enables the users to log into Unified CM Administration.

Procedure

Step 1 Choose User Management > User Settings > Access Control Group. The Find and List Access Control Groups windows appears.
View user roles, access control groups, and permissions

This section describes how to view the roles, access control groups, and permissions that are assigned to a user who belongs to a specified access control group. Use the following procedure to view the roles, access control groups, and permissions that are assigned to a user in an access control group.

Note:
You can also view user roles by using User Management > Application User (for application users) or User Management > End User (for end users) to view a particular user, and then display the user roles.

Procedure

Step 1 Choose User Management > User Settings > Access Control Group.
The Find and List Access Control Groups window appears.

**Step 2** Find the access control group that has the users for which you want to display assigned roles.

**Step 3** Click the name of the access control group for which you want to view the roles that are assigned to the users. The Access Control Group Configuration window appears for the access control group that you chose. The Users pane shows the users that belong to the access control group.

**Step 4** For a particular user, click the username. The Application User Configuration window (for application users) or End User Configuration window (for end users) appears.

**Step 5** From the Related Links drop-down list box, choose User Privilege Report, and then click Go. For the user that you chose, the following information appears:

a) Access control groups to which the user belongs

b) Roles that are assigned to the user

c) Resources to which the user has access. For each resource, the following information appears:

   - Application
   - Resource
   - Permission (read and/or update)

**Step 6** To return to the user, choose Back to User or Back to Application User in the Related Links drop-down list box, and click Go.

**Related Topics**

- Access control group setup, on page 791
- Find access control group, on page 792
End user phone addition

This chapter provides information about adding and configuring end users at the End User, Phone, DN, and LA Configuration window.

- About end user phone and device addition, page 799
- Add and associate end user and phone, page 802

About end user phone and device addition

In Cisco Unified Communications Manager Administration, use the User Management > User/Phone Add menu path to configure an end user, a phone, and a line appearance in a single addition.

The End User, Phone, DN, and LA Configuration window in Cisco Unified Communications Manager Administration provides a single window that allows you to perform the basic steps that are required to add a new user and assign the user to a new phone. While you add a new end user and associate the end user with a new phone, you can configure a new directory number (DN) and line appearance (LA) information for the new end phone.

The End User, Phone, DN, and LA Configuration window, which does not allow you to enter existing end users, phones, or directory numbers, adds records of the following types:

- End users
- Phones
- Directory numbers
- Device profiles
- Voicemail profile

You can modify end user information only if synchronization with an LDAP server is not enabled. To check whether synchronization with an LDAP server is enabled, choose the System > LDAP > LDAP menu option. In the LDAP System window that displays, ensure that the Enable Synchronizing from LDAP Server check box is not checked. If synchronization is enabled, access to the End User, Phone, DN, and LA Configuration window is blocked.
Administrators can customize the End User, Phone, DN, and LA Configuration window. Fields in the window have the following check boxes next to them, which you can use to customize those fields:

- **Default**—Enter a value in the field, then check the Default check box to make that value the default value. Other users can edit the default value, unless the Read Only check box is checked.
- **Hidden**—Check the Hidden check box to hide the field.
- **Read Only**—Check the Read Only check box to make the field read only.

To save your customization changes, click the Save Settings button. The customizations are system-wide, so all other users will see customizations that you save.

To display all hidden fields in the window, click the Show Hidden Fields button.

### User and device settings

The following table describes the end user and device settings.

**Table 119: User and device settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Information</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>Enter the end user identification name. Cisco Unified Communications Manager does not permit modifying the user ID after it is created. You may use the following special characters: =, +, &lt;, &gt;, #, , &quot;, and blank spaces.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, &lt;, &gt;, #, , &quot;, and blank spaces.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the end user password again.</td>
</tr>
<tr>
<td>PIN</td>
<td>Enter five or more numeric characters for the Personal Identification Number.</td>
</tr>
<tr>
<td>Confirm PIN</td>
<td>Enter the PIN again.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the end user last name. You may use the following special characters: =, +, &lt;, &gt;, #, , &quot;, and blank spaces.</td>
</tr>
<tr>
<td>Middle Name</td>
<td>Enter the end user middle name. You may use the following special characters: =, +, &lt;, &gt;, #, , &quot;, and blank spaces.</td>
</tr>
<tr>
<td>First Name</td>
<td>Enter the end user first name. You may use the following special characters: =, +, &lt;, &gt;, #, , &quot;, and blank spaces.</td>
</tr>
<tr>
<td>Device Associations</td>
<td></td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Product Type | This list box displays the types of devices that are available for association with this end user. From the drop-down list box, choose the type of device to associate with this end user.

MAC Address | Enter a unique MAC address for the new device that you are associating with the new user. The MAC address comprises exactly 12 hexadecimal digits (0 to 9, A to F).

Calling Search Space DN | From the drop-down list box, choose the calling search space for the directory number that you are associating with this user and device.

Calling Search Space Phone | From the drop-down list box, choose the calling search space for the phone that you are associating with this user and device.

External Phone Number Mask | Specify the mask that is used to format caller ID information for external (outbound) calls that are made from the associated device.

- The mask can contain up to 24 characters. Valid characters specify 0 to 9, *, #, and X.
- Enter the literal digits that you want to appear in the caller ID information and use Xs to represent the directory number of the associated device.
- See the following examples: If you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234 if the Use External Phone Number Mask option is checked on the route pattern that is used to make the external call. If you specify a mask of all literal digits, such as 9728135000 to represent a main attendant number, that literal number (9728135000) displays as the caller ID for an external call from any associated device.

Extension | This field represents the primary directory number for the end user. End users can have multiple lines on their phones. Enter an extension for the new user and phone. You may use the following characters: 0 to 9, ?, [, ], +, -, *, ^, #, !.

Route Partition | From the drop-down list box, choose a partition for the directory number that you specified in the Extension field.

Voice Mail Profile | From the drop-down list box, choose a voice-mail profile for the directory number. Choose <None> to use the system default.

Enable Extension Mobility | Check this check box to enable extension mobility. After you have added the new user, you can use the User Management > End User menu option to choose an Extension Mobility profile.
Add and associate end user and phone

The following procedure provides instructions on adding an end user and phone and associating the user and phone with a directory number and device profile.

Procedure

Step 1  Choose User Management > User/Phone Add Add.
The End User, Phone, DN, and LA Configuration window displays.

Note  If LDAP synchronization is enabled, access to this window is blocked.

Note Before you proceed, you can use the links in the Related Links drop-down list box at the top, right of the End User, Phone, DN, and LA Configuration window to determine whether an end user or phone already exists.

To find out which end users already exist, choose Back to Find List Users in the Related Links drop-down list box and click Go. Use the Find and List Users window that displays to search for the end user ID that you plan to add. If the end user ID already exists, you cannot use the User/Phone Add menu option to add this end user.

To find out which phones already exist, choose Back to Find List Phones in the Related Links drop-down list box and click Go. Use the Find and List Phones window that displays to search for the phone that you plan to add. If the phone already exists, you cannot use the User/Phone Add menu option to add this phone.

If you use either of the Related Links, repeat Step 1, on page 802 to return to the End User, Phone, DN, and LA Configuration window.

Step 2  Enter the appropriate settings as described in Table 119: User and device settings, on page 800.

Step 3  When you complete the end user configuration, click Save to add the end user and device.
The end user gets created in the Cisco Unified Communications Manager database.

Related Topics

LDAP system setup, on page 89
End user phone addition, on page 799
This chapter provides information to set up Unified Communications (UC) services.

- **About UC service setup**, page 803
- **Add voicemail service**, page 804
- **Add mailstore service**, page 805
- **Add conferencing service**, page 807
- **Add directory service**, page 809
- **Add IM and Presence service**, page 811
- **Add CTI service**, page 812

## About UC service setup

In Cisco Unified Communications Manager Administration, use the **User Management > User Settings > UC Service** to set up unified communications (UC) services such as voicemail, conferencing, CTI, and IM and Presence.

The UC Service window in Cisco Unified Communications Manager Administration allows you to add, search, display, and maintain information about UC services. You can group UC services into service profiles that you associated with end users. After end users have a service profile, their clients can download this profile for seamless integration with the configured UC services.

You can set up these UC services:

- Voicemail
- Mailstore
- Conferencing
- Directory
- IM and presence
- CTI
**UC service setup tips**

- Port values for UC services must match the available port on the server. Change the port number only if it conflicts with other services.

- Cisco recommends that you use HTTPS as the voicemail transport protocol for Cisco Unity and Cisco Unity Connection.

**Add voicemail service**

**Procedure**

**Step 1** Select User Management > User Settings > UC Service.

**Step 2** Select Add New.

**Step 3** Select Voicemail from the UC Service Type drop-down list.

**Step 4** Enter the voicemail settings in the following fields.

**Table 120: Voicemail settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Type</td>
<td>Select a product type. Available options are Unity and Unity Connection.</td>
</tr>
<tr>
<td></td>
<td>Default setting: Unity.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the voicemail service. Ideally, the voicemail service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description that helps you to distinguish between voicemail services. You can change the description if required. Maximum characters: 100.</td>
</tr>
<tr>
<td>Hostname/IP Address</td>
<td>Enter the address of the voicemail service in one of the following forms:</td>
</tr>
<tr>
<td></td>
<td>• Hostname</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• Fully qualified domain name (FQDN)</td>
</tr>
<tr>
<td></td>
<td>This field value must exactly match the hostname, IP address, or FQDN of the associated voicemail service. If the hostname or IP address of the voicemail service changes, change this field value accordingly.</td>
</tr>
</tbody>
</table>
Add mailstore service

Cisco Jabber clients use the mailstore service for visual voicemail functionality.

Procedure

Step 1
Select User Management > User Settings > UC Service.

Step 2
Select Add New.

Step 3
Select Mailstore from the UC Service Type drop-down list.

Step 4
Enter the mailstore settings in the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enter the port to connect with the voicemail service. Default port: 443. This field value must match the available port on the voicemail service. Change the port number only if it conflicts with other services.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to route voicemail messages securely. Available options: HTTP, HTTPS. Default setting: HTTPS. Tip Cisco recommends that you use HTTPS as the voicemail transport protocol for Cisco Unity and Cisco Unity Connection servers. Only change to HTTP if your network configuration does not support HTTPS.</td>
</tr>
</tbody>
</table>

Step 5
Select Save.
The Add Successful message appears and the voicemail service is created in the Unified CM Database.

What to Do Next
Add mailstore service, on page 805

Related Topics
Feature group template setup, on page 857
Table 121: Mailstore settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC Service Type</td>
<td>Specifies the UC service type as Mailstore.</td>
</tr>
<tr>
<td>Product Type</td>
<td>Specifies the product type as Exchange.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the mailstore service. Ideally the mailstore service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description that helps you to distinguish between mailstore services. You can change the description if required.</td>
</tr>
</tbody>
</table>
| Hostname/IP Address  | Enter the address of the mailstore service in one of the following forms:  
• Hostname  
• IP address  
• FQDN  
This field value must exactly match the hostname, IP address, or FQDN of the associated mailstore service. If the address of the mailstore service changes, change this field value accordingly. |
| Port                 | Specify the port number configured for the service. Default Port: 143 Allowed Values: 1 - 65535  
Note For secure voice messaging with Cisco Unity Connection, use port 7993.  
Note This value must match the available port on the mailstore service. Change the port number only if it conflicts with other services. |
Add conferencing service

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select User Management &gt; User Settings &gt; UC Service.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select Add New.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select Conferencing from the UC Service Type drop-down list box.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enter the conferencing settings in the following fields.</td>
</tr>
</tbody>
</table>

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Protocol         | Select the corresponding protocol to use when Cisco Jabber clients contact this service.  
Available Options: TCP, SSL, TLS, UDP  
Default Setting: TCP, which is the most commonly used network configuration. Change this setting to suit your deployment, Unified CM settings, and security needs.  
**Note** For secure voice messaging with Cisco Unity Connection, use TLS.  |
| Product Type     | Select a product type that applies to your network configuration.  
Available Options: MeetingPlace Classic, MeetingPlace Express, WebEx |
| Name             | Enter the name of the conferencing service. Ideally the service name should be descriptive enough for you to instantly recognize it.  
Maximum characters: 50 (ASCII only).  |

**Step 5** Select Save.

The Add Successful message appears and the mailstore service is created in the Unified CM database.

---

**What to Do Next**

Add more UC services.

Add a service profile.

Associate UC services in a service profile to an end user.

**Related Topics**

Feature group template setup, on page 857

---

**Add conferencing service**
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required.</td>
</tr>
</tbody>
</table>
| Hostname/IP Address | Enter the address of the conferencing service in one of the following forms:  
  • Hostname  
  • IP address  
  • FQDN  
  This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly.  
  Allowed values: Alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_). |
| Port                | Enter the port for the conferencing service so that users can contact the service when they sign in to web conferences.  
  Default Port: 80  
  Allowed Values: 1-65535  
  **Note** Use port 80 for HTTP and port 443 for HTTPS communications.  
  **Note** This value must match the available port on the conferencing service. Change the port number only if it conflicts with other services. |
| Protocol            | Select the protocol to route web conference communications.  
  Available Options: HTTP, HTTPS  
  Default Setting: HTTP. Change this setting to suit your network configuration, IM and Presence settings and security needs as follows:  
  **HTTP**  
  Selects Hypertext Transfer Protocol as the standard method for transferring data between the server, Cisco Jabber, and the browser. Select this option if the Cisco Unified MeetingPlace or the Cisco Unified MeetingPlace Express server does not have SSL enabled.  
  **HTTPS**  
  Selects Hypertext Transfer Protocol over SSL as the method for securely transferring data between the server, Cisco Jabber, and the browser. Select this option if the Unified MeetingPlace or the Unified MeetingPlace Express server has SSL enabled. |
Step 5  Select **Save**.
The Add Successful message appears and the conferencing service is created in the Unified CM database.

### What to Do Next

Add more UC services.
Add a service profile.
Associate UC services in a service profile to an end user.

### Related Topics

- Feature group template setup, on page 857

---

### Add directory service

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select <strong>User Management &gt; User Settings &gt; UC Service</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select <strong>Add New</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select <strong>Directory</strong> from the <strong>UC Service Type</strong> drop-down list box.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enter the directory settings in the following fields.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC Service Type</td>
<td>Specifies directory as the UC service type.</td>
</tr>
<tr>
<td>Product Type</td>
<td>Select a supported directory product type from this list that applies to your network configuration. \ Available Options: Directory, Enhanced Directory \ Default Setting: Directory</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the directory service. Ideally the directory service name should be descriptive enough for you to instantly recognize it. \ Maximum characters: 50 (ASCII only). \ Allowed values: All characters allowed except quotes (&quot;), angle brackets (&lt; &gt;), backslash (), ampersand (&amp;), and percent (%).</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description that helps you to distinguish between directory services. You can change the description if required. \ Allowed values: All characters allowed except quotes (&quot;), angle brackets (&lt; &gt;), backslash (), ampersand (&amp;), and percent (%).</td>
</tr>
</tbody>
</table>
Add directory service

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Hostname/IP Address | Enter the address of the directory service in one of the following forms:  
• Hostname  
• IP address  
• FQDN  
This field must exactly match the hostname, IP address, or FQDN of the associated directory service. If the address of the directory service changes, change this field value accordingly.  
Allowed values: Allowed characters include alphanumeric (a-zA-Z0-9), period (.), backslash (\), dash (-), and underscore (_). |
| Port             | Enter the port for the directory service.  
Default Port: 389  
Allowed Values: 1-65535  
**Note** This value must match the available port on the directory service. Change the port number only if it conflicts with other services. |
| Protocol         | Select the protocol to route communications between the directory service and Cisco Jabber clients.  
Available Options: TCP, UDP, TLS  
Default Setting: TCP. This is the most commonly used network configuration. Change this setting to suit your network configuration, Unified CM settings, and security needs. |

**Step 5** Select **Save**.  
The Add Successful message appears and the directory service is created in the Unified CM database.

**What to Do Next**  
Add more UC services.  
Add a service profile.  
Associate UC services in a service profile to an end user.

**Related Topics**  
Feature group template setup, on page 857
# Add IM and Presence service

**Procedure**

**Step 1** Select User Management > User Settings > UC Service.

**Step 2** Select Add New.

**Step 3** Select **IM and Presence** from the UC Service Type drop-down list.

**Step 4** Enter the IM and Presence settings in the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC Service Type</td>
<td>Specifies IM and Presence as the UC service type.</td>
</tr>
<tr>
<td>Product Type</td>
<td>Select a supported IM and Presence product type from this list that applies to your network configuration.</td>
</tr>
<tr>
<td></td>
<td>Available options: Unified CM (IM and Presence), WebEx (IM and Presence)</td>
</tr>
<tr>
<td></td>
<td>Default setting: Unified CM (IM and Presence)</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the IM and Presence service. Ideally the IM and Presence service name should be descriptive enough for you to recognize it instantly.</td>
</tr>
<tr>
<td></td>
<td>Maximum characters: 50 (ASCII only)</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description that helps you to distinguish between IM and Presence services. You can change the description if required.</td>
</tr>
<tr>
<td>Hostname/IP Address</td>
<td>Enter the address of the IM and Presence service in one of the following forms:</td>
</tr>
<tr>
<td></td>
<td>• Hostname</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• DNS SRV</td>
</tr>
<tr>
<td></td>
<td>Allowed values: Allowed characters include alphanumeric (a-zA-Z0-9), period (.), backslash (), dash (-), and underscore (_).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field value must exactly match the host name, IP address, or DNS SRV of the associated IM and Presence service. If the address of the IM and Presence service changes, change this field value accordingly.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> Cisco recommends DNS SRV to help the client find the correct IM and Presence service for the user.</td>
</tr>
</tbody>
</table>
Step 5  Select Save.
The Add Successful message appears and the IM and Presence service is created in the Unified CM database.

What to Do Next
Add more UC services.
Add a service profile.
Associate UC services in a service profile to an end user.

Related Topics
Feature group template setup, on page 857

Add CTI service
Soft clients use the CTI service for deskphone control

Procedure

Step 1  Select User Management > User Settings > UC Service.
Step 2  Select Add New.
Step 3  Select CTI from the UC Service Type drop-down list box.
Step 4  Enter the computer telephone integration (CTI) settings in the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC Service Type</td>
<td>Specifies CTI as the UC service type.</td>
</tr>
<tr>
<td>Product Type</td>
<td>Specifies CTI as the product type.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the CTI service. Ideally the CTI service name should be descriptive enough for you to instantly recognize it. Maximum characters: 50 (ASCII only).</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description that helps you to distinguish between CTI services when you have more than one configured. You can change the description if required.</td>
</tr>
</tbody>
</table>
**Field** | **Description**  
--- | ---  
Hostname/IP Address | Enter the address of the CTI service in one of the following forms:  
- Hostname  
- IP address  
- FQDN  
This field must exactly match the hostname, IP address, or FQDN of the associated CTI service. If the address of the CTI service changes, change this field value accordingly.  

Port | Enter the port for the CTI service.  
Default port: 2748  
Allowed ports: 1-65535  
**Note** This value must match the available port on the CTI service. Change the port number only if it conflicts with other services.  

Protocol | Specifies TCP as the default protocol.  

---  

**Step 5**  
Select **Save**.  
The Add Successful message appears and the CTI service is created in the Unified CM database.  

**What to Do Next**  
Add more UC services.  
Add a service profile.  
Associate UC services in a service profile to an end user.  

**Related Topics**  
- Feature group template setup, on page 857
Service profile setup

This chapter contains information to set up service profiles.

- About service profile setup, page 815
- Add service profile, page 819

About service profile setup

In Cisco Unified Communications Manager (Unified CM) Administration, use the User Management > User Settings > Service Profile menu path to set up service profiles from existing unified communications (UC) services.

The Service Profile window in Unified CM allows you to add, search, display, and maintain information about service profiles that you can assign to end users.

Note

If you want a listing of the users associated with a service profile, you can select Dependency Records from the Related Links drop-down list box in the upper right corner.

Service profile setup tips

- Before you create service profiles, you must configure unified communications (UC) services.
- If you upgrade the system from a pre-9.0 Cisco Unified Presence installation, the existing service profiles are migrated from Cisco Unified Presence to Unified CM. You do not lose your service profile settings after you upgrade.
- Migrated service profiles have auto-generated names. You can change them at a later point.
- Prior to Cisco Unified CM IM and Presence Service Release 9.0(1), service profile data used to be editable from Cisco Unified Presence Administration under the Application > CUPC/Cisco Jabber menu.
- When you configure the IM and Presence UC service, you cannot mix and match product types for the primary, secondary, and tertiary servers. However, you can mix and match the other services.
- If your primary voicemail server is Cisco Unity, you must configure the primary voicemail and primary mailstore servers.

- If your primary voicemail server is Cisco Unity Connection, you do not need to configure a primary voicemail server but you must select a primary mailstore server.

- The primary, secondary, and tertiary server drop-down lists contain the UC services that you previously configured on the UC Services window. Change the servers to suit your network configuration.

- When you use an IM-only client, you cannot set up the service profiles with CTI on Cisco Unified Communications Manager or CCMIP on IM and Presence as it causes high CPU activity on the Cisco Unified Communications Manager and IM an Presence servers.

**Service profile settings**

The following table lists and describes the service profile field settings.

*Table 123: Service profile settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Profile Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the service profile. Ideally the service profile name should be descriptive enough for you to instantly recognize it. This name is visible on the End User settings window. Maximum characters: 50 (ASCII only). Allowed Values: All characters allowed except quotes (&quot;), angle brackets (&lt; &gt;), backslash (), ampersand (&amp;), and percent (%).</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description that helps you to distinguish between service profiles when you have more than one configured. You can change the description if required. Allowed Values: All characters allowed except quotes (&quot;), angle brackets (&lt; &gt;), backslash (), ampersand (&amp;), and percent (%)</td>
</tr>
<tr>
<td>Make this the default service profile for the system</td>
<td>Check this check box to make this service profile the default option for the system. <strong>Note</strong> If you specify a default service profile, end users that do not have an associated service profile automatically inherit the default service profile settings.</td>
</tr>
<tr>
<td><strong>Voicemail Profile</strong></td>
<td></td>
</tr>
<tr>
<td>Primary</td>
<td>Select the primary voicemail server with which you want to associate this service profile. This drop-down list contains the voicemail servers that you previously configured on the UC Services window.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Select a secondary voicemail server, if applicable.</td>
</tr>
<tr>
<td>Tertiary</td>
<td>Select a tertiary voicemail server, if applicable.</td>
</tr>
</tbody>
</table>
### Mailstore Profile

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Select a primary mailstore server. This drop-down list contains the mailstore servers that you previously configured on the UC Services window.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Select a secondary mailstore server, if applicable.</td>
</tr>
<tr>
<td>Tertiary</td>
<td>Select a tertiary mailstore server, if applicable.</td>
</tr>
</tbody>
</table>

### Conferencing Profile

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Select a primary conferencing server. This drop-down list contains the conferencing servers that you previously configured on the UC Services window.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Select a secondary conferencing server, if applicable.</td>
</tr>
<tr>
<td>Tertiary</td>
<td>Select a tertiary conferencing server, if applicable.</td>
</tr>
</tbody>
</table>

#### Server Certificate Verification

**Default:** Any

Specify how the conferencing server associated with this profile supports TLS connections. This setting is for TLS verification of the conferencing servers listed for this conferencing profile.

Select from the following options:

- **Any Certificate**
  - Cisco Jabber accepts all valid certificates.

- **Self Signed or Keystore**
  - Cisco Jabber accepts the certificate if the certificate is self-signed, or the signing Certificate Authority certificate is in the local trust store.
  
  **Note** A keystore is a file that stores authentication and encryption keys.

- **Keystore Only**
  - Cisco Jabber accepts only certificates that are defined in the keystore. You must import the certificate or its Certificate Authority signing certificate into the local trust store.

### Directory Profile

---

*Cisco Unified Communications Manager Administration Guide, Release 9.1(1)*
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Primary                    | Select a primary directory server. This drop-down list contains the directory servers that you previously configured on the UC Services window.  
**Note** If you select User Data Service (UDS) for directory integration, then you can use UDS for directory searches without selecting any primary, secondary, or tertiary servers. Clients connect to UDS using DNS/SRV.  
**Tip** Instead of or in addition to UDS, you can specify primary, secondary, tertiary basic or advanced LDAP UC services, because some clients that use these may not support UDS. |
| Secondary                  | Select a secondary directory server, if applicable. If you do not set up any backup directory servers, you cannot perform directory searches for Cisco Jabber clients if the first server fails.                                     |
| Tertiary                   | Select a tertiary directory server, if applicable. If you do not configure any backup directory servers, you cannot perform directory searches for Cisco Jabber clients if the first server fails.                                                  |

**IM and Presence Profile**

| Primary                    | Select a primary IM and Presence server. This drop-down list contains the IM and Presence servers that you previously configured on the UC Services window.  
**Note** An IM and Presence profile cannot mix the IM and Presence server and Webex Presence server. |
| Secondary                  | Select a secondary IM and Presence server, if applicable.                                                                                                                                                |
| Tertiary                   | Select a tertiary IM and Presence server, if applicable.                                                                                                                                                  |

**CTI Profile**

| Primary                    | Select a primary CTI server. This drop-down list contains the CTI servers that you previously configured on the UC Services window.                                                                       |
| Secondary                  | Select a secondary CTI server, if applicable.                                                                                                                                                             |
| Tertiary                   | Select a tertiary CTI server, if applicable.                                                                                                                                                              |

**Related Topics**

Add service profile, on page 819
Add service profile

Procedure

Step 1  In Unified CM Administration, select User Management > User Settings > Service Profile
The Find and List window appears.

Step 2  Select Add New.

Step 3  Enter settings for the service profile fields. See About service profile setup, on page 815.

Step 4  Select Save.
The Add Successful message appears and the service profile gets created in the Cisco Unified CM database.

Related Topics

- About UC service setup, on page 803
- About service profile setup, on page 815
Add service profile
Universal device template setup

This chapter contains information to set up universal device templates.

- Universal Device Template setup, page 821

Universal Device Template setup

In Cisco Unified Communications Manager Administration, use the User Management > Quick User/Phone Add > Universal Device Template menu path to set up universal device templates (UDTs) that you can apply to any device, such as a phone, RDP, or EM Profile, that you create later.

UDTs are templates that you create to apply to any device. Administrators can view all device-related settings in one simple interface and apply these settings to any device. UDTs use tokens, which are variables in specific fields that fill in information (such as an employee name) automatically. These templates ease administrative tasks that relate to setting up users and devices and keep a range of device settings on one central, customizable interface.

Universal Device Template settings

Note

The UDT sections in this window may appear in a different order than the following table indicates. To change the order of these settings, use the User Management > Quick User/Phone Add > Universal Device Templates Display Preference menu.

Note

To make the window easier to view, the template sections are collapsed by default. Expand sections that you need as you review the template setup process. Select the Expand All button on the bottom of the window to expand all sections. To customize the Universal Device Templates window, see "Universal device template display preference setup"
The UDT sections in this window may appear in a different order than the following table indicates. To change the order of these settings, use the User Management > Quick User/Phone Add > Universal Device Templates Display Preference menu.

To make the window easier to view, the template sections are collapsed by default. Expand sections that you need as you review the template setup process. Select the Expand All button on the bottom of the window to expand all sections. To customize the Universal Device Template window, see “Universal device template display preference setup”.

This table describes the available settings in the Universal Device Template window.

**Table 124: Universal Device Template settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Template Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify this UDT.</td>
</tr>
<tr>
<td><strong>Required and Frequently Entered Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Enter the purpose of the UDT. You can enter the functional rule of a group of users or the key features enabled in the template.</td>
</tr>
<tr>
<td>Tip</td>
<td>You can click the pencil icon to place tokens in the description. Tokens are variables that are replaced with actual values, after you create this UDT. You can select the available elements from the list (such as User First Name). For example, the token &quot;/Lastname/s desk phone&quot; becomes &quot;Smith's desk phone&quot; for a user with the last name &quot;Smith.&quot;</td>
</tr>
<tr>
<td>Note</td>
<td>When you insert the device with this template, the element in the description is propagated based on the actual device or user information.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Select the device pool for the UDT. The device pool defines sets of common characteristics for this UDT, such as region, date/time group, softkey template, and MLPP information.</td>
</tr>
</tbody>
</table>
Universal Device Template setup

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Security Profile| Choose the device security profile for the UDT. The security profile for the UDT is model and protocol independent.  
**Note**  You can only select a model-independent security profile for a UDT.  
To identify the settings that the profile contains, see the System > Security Profile > Phone Security Profile menu.  
**Note**  If you enable the security feature for a template, the security setting is applied to the phone inserted with this template only when the phone supports all of the following security features.  
1  Security Authentication  
2  Security Encryption  
3  File Encrypt  
Otherwise you insert the phone with the default non-secure security profile with the same model and device protocol of the inserted phone.  
For more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings, see the Cisco Unified Communications Manager Security Guide. |
| SIP Profile            | Select the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information such as registration and keepalive timers, media ports, and Do Not Disturb control. |
| Phone Button Template  | Select the appropriate phone button template for the UDT. The phone button template determines the behavior of buttons, and identifies which feature (such as line and speed dial) is used for each button.  
**Note**  You must select a phone button template before you can expand the Phone Button Configuration field.  
**Note**  You can only assign universal phone button templates to a UDT. |
| **Phone Buttons Configuration** | Use this section to view and change the settings for the universal phone button template. This section lists the configurable buttons for the phone button template that you select in the Phone Button Template field.  
You can update a universal phone button template to add or remove features; add or remove lines and speed dials; or assign features, lines, and speed dials to different buttons on the phone that you add after you create the UDT. You can change the button labels in the default phone button templates, but you cannot change the function of the buttons in the default templates.  
**Note**  If you update a phone template, be sure to inform affected users of the changes. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Appearance</td>
<td></td>
</tr>
<tr>
<td>Directory Number</td>
<td>Select a directory number (DN) from the drop-down list box. After you create a device with this UDT, the DN will exist on the newly created device automatically.</td>
</tr>
<tr>
<td>Line Label</td>
<td>If left blank, this defaults to the line number. If you desire a different label for the line on the phone, you can enter it here.</td>
</tr>
<tr>
<td>Tip</td>
<td>You can use tokens (pencil icon) to enter the line label.</td>
</tr>
<tr>
<td>Display (Caller ID)</td>
<td>Leave this field blank to have the system display the extension. Use a maximum of 30 alphanumeric characters. Typically, use the username or the directory number (if using the directory number, the person receiving the call may not see the proper identity of the caller).</td>
</tr>
<tr>
<td>Tip</td>
<td>You can use tokens (pencil icon) to enter the display.</td>
</tr>
<tr>
<td>Ring Setting When Phone is Idle *</td>
<td>Use this field to set up the ring setting for this UDT for the line appearance when an incoming call is received and no other active calls exist on that device. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Use system default</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td></td>
<td>• Flash only</td>
</tr>
<tr>
<td></td>
<td>• Ring once</td>
</tr>
<tr>
<td></td>
<td>• Ring</td>
</tr>
<tr>
<td>Ring Setting When Phone is in Use</td>
<td>From the drop-down list box, select the ring setting that is used for this UDT when it has an active call on a different line. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Use system default</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td></td>
<td>• Flash only</td>
</tr>
<tr>
<td></td>
<td>• Ring once</td>
</tr>
<tr>
<td></td>
<td>• Ring</td>
</tr>
<tr>
<td></td>
<td>• Beep only</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Visual Message Waiting Indicator Policy *</td>
<td>Enter the external phone number (or mask) that is used to send Caller ID information for this UDT. You can enter a maximum of 24 number, the international escape character +, and &quot;X&quot; characters. The Xs represent the directory number and must appear at the end of the pattern. For example, if you specify a mask of 972813XXXX, an external call from extension 1234 displays a caller ID number of 9728131234.</td>
</tr>
</tbody>
</table>
| Audible Message Waiting Indicator Policy *          | Use this field to configure the ring setting for the line appearance when an incoming call is received and no other active calls exist on that device. Select one of the following options:  
  • Use system default  
  • Disable  
  • Flash only  
  • Ring once  
  • Ring                                                                                                                                 |

Cisco Unified Communications Manager Administration Guide, Release 9.1(1)
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Options *</td>
<td>This field determines the recording option on the line appearance of an agent. The default recording option is Call Recording Disabled.</td>
</tr>
<tr>
<td></td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td>Call Recording Disabled</td>
<td>You cannot record call that you make on this line appearance.</td>
</tr>
<tr>
<td>Selective Call Recording Enabled</td>
<td>You can record calls that you make on this line appearance by using a softkey or programmable line key that is assigned to the device, a CTI-enabled application, or both interchangeably. Selective recording supports two modes:</td>
</tr>
<tr>
<td>Silent recording</td>
<td>Call recording status is not reflected on the Cisco IP device display. Silent recording is typically used in a call center environment to allow a supervisor to record an agent call. A CTI-enabled application running on the supervisor desktop is generally used to start and stop the recording for an agent-customer call.</td>
</tr>
<tr>
<td>User recording</td>
<td>User recording—Call recording status is reflected on the Cisco IP device display. You can start or stop a recording by using a softkey, programmable line key, or CTI-enabled application running on the user desktop. To enable user recording, add the Record softkey or programmable line key to the UDT. Do not add the Record softkey if you only want silent recording.</td>
</tr>
</tbody>
</table>

When the recording option is set to either Automatic Call Recording Enabled or Selective Call Recording Enabled, you can associate the line appearance with a recording profile. When automatic recording is enabled, start- and stop-recording requests using a softkey, programmable line key, or CTI-enabled application are rejected.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Profile</td>
<td>This field determines the recording profile on the line appearance of an agent. Choose an existing recording profile from the drop-down list box. To create a recording profile, use the Device &gt; Device Settings &gt; Recording Profile menu option. The default value specifies None.</td>
</tr>
<tr>
<td>Call Pickup Group Audio Alert Setting (Phone Active)</td>
<td>This field determines the type of notification an incoming call sends to members of a call pickup group. If the called phone does not answer, the phones in the call pickup group that are busy will either hear a beep (beep beep) or hear nothing (disabled).</td>
</tr>
<tr>
<td></td>
<td><strong>Use System Default</strong></td>
</tr>
<tr>
<td></td>
<td>The setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Busy Station determines the value of this field.</td>
</tr>
<tr>
<td></td>
<td><strong>Disable</strong></td>
</tr>
<tr>
<td></td>
<td>No alert is sent to member of the call pickup group.</td>
</tr>
<tr>
<td></td>
<td><strong>Beep Only</strong></td>
</tr>
<tr>
<td></td>
<td>A beep beep is sent to members of the call pickup group.</td>
</tr>
<tr>
<td>Call Pickup Group Audio Alert Setting (Phone Idle)</td>
<td>This field determines the type of notification an incoming call sends to members of a call pickup group. If the called phone does not answer, the phones in the call pickup group that are idle will either hear a short ring (ring once) or hear nothing (disabled).</td>
</tr>
<tr>
<td></td>
<td><strong>Use System Default</strong></td>
</tr>
<tr>
<td></td>
<td>The setting of the Cisco CallManager service parameter Call Pickup Group Audio Alert Setting of Idle Station determines the value of this field.</td>
</tr>
<tr>
<td></td>
<td><strong>Disable</strong></td>
</tr>
<tr>
<td></td>
<td>No alert is sent to members of the call pickup group.</td>
</tr>
<tr>
<td></td>
<td><strong>Ring Once</strong></td>
</tr>
<tr>
<td></td>
<td>A short ring is sent to members of the call pickup group.</td>
</tr>
</tbody>
</table>
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. Choose an existing calling search space from the drop-down list box.

The default value specifies None.

### SpeedDial

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Calling Search Space</td>
<td>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. Choose an existing calling search space from the drop-down list box. The default value specifies None.</td>
</tr>
<tr>
<td>(number from 1 to 199 in the left column)</td>
<td>This column identifies the speed-dial button (for example, 1, 2, 3, or 4) or the abbreviated-dial index for abbreviated dial.</td>
</tr>
<tr>
<td>Number</td>
<td>Enter the number that you want the system to dial when the user presses the speed-dial button. You can enter digits 0 through 9, *, #, and +, which is the international escape character. For a Pause in Speed Dial, you can enter comma (,) which can act as a delimiter as well as other pause before sending DTMF digits.</td>
</tr>
<tr>
<td>Label</td>
<td>Enter the text that you want to display for the speed-dial button or abbreviated-dial number. <strong>Note</strong> If you are configuring a Pause in Speed Dial, you must add a label so that FAC, CMC, and DTMF digits are not displayed on the phone screen.</td>
</tr>
</tbody>
</table>

### BLF SpeedDial

With the BLF Presence feature, a watcher can monitor the status of the presence entity (also called presentity). When you configure BLF/SpeedDial buttons, the presence entity appears as a speed dial on the device of the watcher.

The following section describes the settings that you configure for BLF/SpeedDial buttons.
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-Unified CM directory numbers as BLF/SpeedDial buttons, enter the directory number in this field.

For this field, enter only numerals, asterisks (*), and pound signs (#).

**Note** If you configure the Destination field, do not select an option from the Directory Number drop-down list box. If you select an option from the Directory Number drop-down list box after you configure the Destination, Unified CM deletes the Destination configuration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Perform one of the following tasks to configure a SIP URI or a directory number as a BLF/SpeedDial button:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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-Unified CM directory numbers as BLF/SpeedDial buttons, enter the directory number in this field.</td>
</tr>
<tr>
<td></td>
<td>For this field, enter only numerals, asterisks (*), and pound signs (#).</td>
</tr>
<tr>
<td>Directory Number</td>
<td>The Directory Number drop-down list box displays a list of directory numbers that exist in the Unified CM database. Configure this setting only if you did not configure the Destination field.</td>
</tr>
<tr>
<td></td>
<td>For a UDT that runs either SCCP or SIP, select 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.</td>
</tr>
<tr>
<td></td>
<td>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>BLF Directed Call Park</td>
<td>The Directory Number drop-down list box displays a list of directory numbers that exist in the Unified CM database.</td>
</tr>
<tr>
<td></td>
<td>For a UDT that runs either SCCP or SIP, select the number (and corresponding partition, if it appears) that you want the system to dial when the user presses the speed-dial button; for example, 6002 in 3. Directory numbers that appear without specific partitions belong to the default partition</td>
</tr>
</tbody>
</table>
### Universal Device Template setup

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Enter the text that you want to appear for the BLF/Directed Call Park button. This field supports internationalization. If your phone does not support internationalization, the system uses the text that appears in the Label ASCII field.</td>
</tr>
<tr>
<td>Service URL</td>
<td></td>
</tr>
<tr>
<td>Button Service</td>
<td>Enter the name of the service. If the service is not marked as an enterprise subscription, the service name appears in areas where you can subscribe to a service; for example, under Unified CM User Options. Enter up to 32 characters for the service name.</td>
</tr>
<tr>
<td>Label</td>
<td>Enter the text that you want to appear for the Service URL button.</td>
</tr>
<tr>
<td>Device Settings</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>Enter a name to identify the device that uses this UDT. For device names that are not based on a MAC address, as a general rule, you can enter 1 to 15 characters comprised of alphanumeric characters (a-z, A-D, 0-9). In most cases, you can also enter dot (.), dash (-), and underscore (_).</td>
</tr>
<tr>
<td>Owner User ID</td>
<td>From the drop-down list box, select the User ID that you want to assign as the device owner for devices that use this UDT. By default, this field is set to the <strong>Current Device Owner's User ID</strong>. If this option is configured, when you use this UDT to create a device in the Quick User/Phone Add menu, the user ID under which you create the device is assigned as the device owner. In addition, if self provisioning is enabled for a user, when that user logs into the device for the first time, the device is created automatically with that user’s user ID as the device owner. You may also select a specific user ID as the device owner for all devices that use this UDT. If you choose this option, when you use this UDT to create a device in the Quick User/Phone Add menu, regardless of which user you use to create the device, Cisco Unified Communications Manager assigns the user ID in the UDT Owner User ID drop-down list box as the device owner.</td>
</tr>
<tr>
<td>Mobility User ID</td>
<td>From the drop-down list box, select the user ID of the assigned mobility user. You can either select a user ID to own all devices created using this UDT, or select <strong>Current Device Owner's User ID</strong> to have the user who the devices are created for (using this UDT) as the owner of the device. <strong>Tip</strong> Assign the element that represents the user ID to the UDT to associate the UDT to the user or owner ID.</td>
</tr>
</tbody>
</table>
### Join Across Lines

From the drop-down list box, enable or disable the Join Across Lines feature or select Default to use the service parameter setting.

- **Off**
  - This setting disables the Join Across Lines feature.
- **On**
  - This setting enables the Join Across Lines feature.
- **Default**
  - This setting uses the Join Across Lines setting that is in the service parameter.

### Always Use Prime Line

From the drop-down list box, choose one of the following options:

- **Off**
  - When a device is idle and receives a call on any line, a user answers the call from the line on which the call is received.
- **On**
  - When a device is idle (off hook) and receives a call on any line, the primary line is chosen for the call. Calls on other lines continue to ring, and the user must select those other lines to answer these calls.
- **Default**
  - Unified CM uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
From the drop-down list box, choose one of the following options:

**On**
- If a device is idle, the primary line becomes the active line for retrieving voice messages when a user presses the Messages button.

**Off**
- If a device is idle, pressing the Messages button automatically dials the voice-messaging system from the line that has a voice message. Unified CM always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when a user presses the Messages button.

**Default**
- Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

From the drop-down list box, enable or disable the Single Button Barge/cBarge feature for this UDT or choose Default to use the service parameter setting.

**Off**
- This setting disables the Single Button Barge/cBarge feature; however, the regular Barge or cBarge features still work.

**Barge**
- This setting enables the Single Button Barge feature.

**cBarge**
- This setting enables the Single Button cBarge feature.

**Default**
- Uses the Single Button Barge/cBarge setting that is in the service parameter.

For more information, see “Barge and Privacy” in the *Cisco Unified Communications Manager Features and Services Guide.*
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>For privacy on this UDT, select <strong>On</strong> in the Privacy drop-down list box. For more configuration information, see “Barge and Privacy” in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
<tr>
<td>Built in Bridge</td>
<td>Enables or disables the built-in conference bridge for the barge feature (select <strong>On</strong>, <strong>Off</strong>, or <strong>Default</strong>). For more information, see “Barge and Privacy” in the <em>Cisco Unified Communications Manager Features and Services Guide</em> and the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
<tr>
<td>Allow Control of Device from CTI</td>
<td>Check this check box to allow CTI to control and monitor this UDT. If the associated directory number specifies a shared line, you should check the check box as long as at least one associated device specifies a combination of device type and protocol that CTI supports.</td>
</tr>
<tr>
<td>Hotline Device</td>
<td>Check this check box to enable Hotline device for this UDT. Hotline devices can only connect to other Hotline devices. This feature is an extension of PLAR, which configures a device 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>
<tr>
<td>Logged into Hunt Group</td>
<td>This check box indicates that this UDT is currently signed in to a hunt list (group). When this UDT is added to a hunt list, the administrator can sign the user in or out by checking or unchecking this check box. Users use the softkey on a device to sign in or out of the hunt list.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry Video Call as Audio</td>
<td>This check box applies only to video endpoints that receive a call. If devices using this UDT receive a call that does not connect as video, the call tries to connect as an audio call. By default, the system checks this check box to specify that devices on this UDT should immediately retry a video call as an audio call (if it cannot connect as a video call) prior to sending the call to call control for rerouting. If you uncheck this check box, a video call that fails to connect as video does not try to establish as an audio call. The call then fails to call control, and call control routes the call via Automatic Alternate Routing (AAR), route list, or hunt list.</td>
</tr>
<tr>
<td>Ignore Presentation Indicators (internal calls only)</td>
<td>Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Unified CM ignores any presentation restriction that is received for internal calls. 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 connected line display information for each call. For more information about call display restrictions, see the “Call Display Restrictions” chapter in the <em>Cisco Unified Communications Manager Features and Services Guide.</em></td>
</tr>
<tr>
<td>Enable Extension Mobility</td>
<td>Check this check box if to allow this UDT to support extension mobility.</td>
</tr>
<tr>
<td>Require Off-Premise Location</td>
<td>Check this check box if the device inserted with this template requires off-premise location update upon the registration. Off-premise location update is required when the device location cannot be detected automatically by Cisco Emergency Responder. Check this check box only for the template that remote or mobile devices use, which have frequent location change.</td>
</tr>
</tbody>
</table>

### Device Routing

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Dial Rules</td>
<td>If required, select the appropriate SIP dial rule. SIP dial rules provide local dial plans for this UDT, so users do not have to press a key or wait for a timer before the call is processed. Leave the SIP Dial Rules field set to <strong>None</strong> if you do not want dial rules to apply to this UDT. This means that the user must use the dial softkey or wait for the timer to expire before the call gets processed.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
Calling Search Space | From the drop-down list box, select the appropriate calling search space (CSS). A CSS comprises a collection of partitions that are searched to determine how a dialed number should be routed. The calling search space for this UDT and the calling search space for the directory number are used together. The directory number CSS takes precedence over the device CSS. For more information, see “Partitions and Calling Search Spaces” in the *Cisco Unified Communications Manager System Guide.*

Calling Party Transformation CSS for Inbound Calls | This setting allows you to localize the calling party number on this UDT for inbound calls. Make sure that the Calling Party Transformation CSS that you select contains the calling party transformation pattern that you want to assign to this UDT. **Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS for Inbound Calls as None, the transformation does not match and is not applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

Calling Party Transformation CSS for Outbound Calls | This setting allows you to localize the calling party number on this UDT for outbound calls. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this UDT. **Tip** Before the call occurs, the UDT must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS for Outbound Calls as None, the transformation does not match and is not applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

Rerouting Calling Search Space | From the drop-down list box, select a calling search space to use for rerouting. The rerouting calling search space of the referrer is used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the 405 Method Not Allowed message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| SUBSCRIBE Calling Search Space                 | Supported with the BLF Presence feature, the SUBSCRIBE calling search space determines how Unified CM routes BLF presence requests that come from this UDT. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the UDT.  
From the drop-down list box, select the SUBSCRIBE calling search space to use for BLF presence requests for this UDT. All calling search spaces that you configure in Unified CM Administration appear in the SUBSCRIBE Calling Search Space drop-down list box.  
If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. |
| Use Device Pool Calling Party Transformation CSS for Inbound Calls | To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this UDT, check this check box. If you do not check this check box, this UDT uses the Calling Party Transformation CSS setting for inbound calls. |
| Use Device Pool Calling Party Transformation CSS for Outbound Calls | To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this UDT, select this check box. If you do not select this check box, the UDT uses the Calling Party Transformation CSS for outbound calls that you selected in the Phone Configuration window. |
| **Phone Settings**                              |                                                                                                                                                                                                         |
| Common Profile                                  | From the drop-down list box, select a common phone profile from the list of available common phone profiles. Select View Details for specific details about each common phone profile. |
| Common Device Configuration                     | From the drop-down list box, you can select a common device configuration that was configured in the Common Device Configuration window. Select View Details for specific details about each common device configuration. |
| Softkey Template                                | From the drop-down list box, select a softkey template. Leave the softkey template set to <None> to use the softkey template configured in the assigned Common Phone Profile. |
From the drop-down list box, select a feature control policy that has already been configured in the Feature Control Policy configuration window (Device > Device Settings > Feature Control Policy).

Leave the softkey template set to <None> to use the feature control policy configured in assigned Common Phone Profile.

**Phone Personalization**

The Phone Personalization setting allows you to enable this UDT so that it works with Phone Designer. Phone designer is a Cisco Unified Communications widget that allows a user to customize the wallpaper and ring tones on a device.

From the Phone Personalization drop-down list box, select one of the following options:

- **Disabled**
  
  The user cannot customize this UDT by using Phone Designer.

- **Enabled**
  
  The user can use Phone Designer to customize this UDT.

- **Default**
  
  This UDT uses the configuration from the Phone Personalization enterprise parameter.

**Note** You must install and configure Phone Designer, so a user can customize the device.

**Protocol Settings**

**MTP Preferred Originating Codec**

From the drop-down list box, select the codec to use if a media termination point is required for SIP calls.

**Digest User**

Select an end user that you want to associate with this UDT for this setting that is used with digest authentication (SIP security).

**Note** Ensure that you configured digest credentials for the user that you choose, as specified in the End User setting window.

After you save the UDT and apply the setup update to the device, the digest credentials for the user is added to the phone configuration file.

For more information about digest authentication, see the *Cisco Unified Communications Manager Security Guide*.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Call Rollover</td>
<td>Use this setting if you are creating this UDT for a Cisco Unified IP Phone 7931.</td>
</tr>
<tr>
<td></td>
<td><strong>No Rollover</strong></td>
</tr>
<tr>
<td></td>
<td>Conference and transfer do not work in this mode. If a user attempts to use either of these features, the phone status displays as Error Pass Limit.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Choose this setting only if you need to support CTI applications.</td>
</tr>
<tr>
<td></td>
<td><strong>Rollover Within Same DN</strong></td>
</tr>
<tr>
<td></td>
<td>Conferences and call transfers complete by using the same directory number (on different lines). For example, consider a phone that has directory number 1506 that is assigned to both Line 6 and 7. The user has an active call on Line 6 and decides to transfer the call. When the user presses the Transfer button, the call on Line 6 gets placed on hold, and a new call initiates on Line 7 to complete the transfer.</td>
</tr>
<tr>
<td></td>
<td><strong>Rollover to any line</strong></td>
</tr>
<tr>
<td></td>
<td>Conferences and call transfers complete by using a different directory number and line than the original call. For example, consider a phone that has directory number 1507 assigned to Line 8 and directory number 1508 assigned to Line 9. The user has an active call on Line 8 and decides to transfer the call. When the user presses the Transfer button, the call on Line 8 is placed on hold, and a new call initiates on Line 9 to complete the transfer.</td>
</tr>
<tr>
<td>Media Termination Point Required</td>
<td>Check this check box if you want to use an MTP to implement features that H.323 does not support (such as hold and transfer). Uncheck this check box if you do not want to use an MTP to implement features.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Check this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source.</td>
</tr>
<tr>
<td></td>
<td>If you check this check box to require an MTP and a device becomes the endpoint of a video call, the call will be audio only.</td>
</tr>
<tr>
<td>Unattended Port</td>
<td>Check this check box to indicate an unattended port on this UDT.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Require DTMF Reception</td>
<td>Check this check box to require DTMF reception for this UDT.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.</td>
</tr>
</tbody>
</table>

**IP Phone Services Subscription**

Select the **Subscribe** button and select the service. If the service is not marked as an enterprise subscription, the service name appears in areas where you can subscribe to a service.

Enter up to 128 characters for the service name.

For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file.

**Note** You must configure IP Phone services and save them before you can configure Service URL Buttons.

**Note** Unified CM allows you to create two or more IP phone services with identical names. Cisco recommends that you do not do so unless most or all phone users are advanced, or unless an administrator always configures the IP phone services. Be aware that if AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services.

**Security Settings**

General Security Settings
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Trusted Relay Point</td>
<td>From the drop-down list box, enable or disable whether Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Select one of the following values:</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this value, the UDT uses the Use Trusted Relay Point setting from the common device configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Off</strong></td>
</tr>
<tr>
<td></td>
<td>Select this value to disable the use of a TRP with this UDT. This setting overrides the Use Trusted Relay Point setting in the common device configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>On</strong></td>
</tr>
<tr>
<td></td>
<td>Select this value to enable the use of a TRP with this UDT. This setting overrides the Use Trusted Relay Point setting in the common device configuration.</td>
</tr>
</tbody>
</table>

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point.

Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVP Agent).

If both TRP and MTP are required for the endpoint, TRP is used as the required MTP. For information about call behavior, see "TRP Insertion in Cisco Unified Communications Manager" in the *Cisco Unified Communications Manager System Guide*.

If both TRP and RSVP Agent are needed for the endpoint, Unified CM first tries to find an RSVP Agent that can also be used as a TRP.

If both TRP and transcoder are needed for the endpoint, Unified CM first tries to find a transcoder that is also designated as a TRP.

For more information about network virtualization and trusted relay points, see the Trusted Relay Point section and its subtopics in the "Media Resource Management" chapter of the *Cisco Unified Communications Manager System Guide*.
Check this checkbox to designate this UDT as protected, which enables a device to play a 2-second tone to notify the user when a call is encrypted and both devices are configured as protected. The tone plays for both parties when the call is answered. The tone does not play unless both devices are protected and the call occurs over encrypted media.

This setting represents only one of several configuration requirements for the secure indication tone to play. For more information about the secure indication tone feature and the configuration requirements, see the *Cisco Unified Communications Manager Security Guide*.

**Note**  If you check this check box and the system determines that the call is not encrypted, a device plays an indication tone to alert the user that the call is not protected.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected Device</td>
<td>Check this check box to designate this UDT as protected, which enables a device to play a 2-second tone to notify the user when a call is encrypted and both devices are configured as protected. The tone plays for both parties when the call is answered. The tone does not play unless both devices are protected and the call occurs over encrypted media. This setting represents only one of several configuration requirements for the secure indication tone to play. For more information about the secure indication tone feature and the configuration requirements, see the <em>Cisco Unified Communications Manager Security Guide</em>. <strong>Note</strong>  If you check this check box and the system determines that the call is not encrypted, a device plays an indication tone to alert the user that the call is not protected.</td>
</tr>
</tbody>
</table>

Certificate Authority Proxy Function (CAPF) Settings
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Mode</td>
<td>This field allows you to choose the authentication method that this UDT uses during the CAPF certificate operation. From the drop-down list box, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td><strong>By Authentication String</strong></td>
</tr>
<tr>
<td></td>
<td>Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the UDT.</td>
</tr>
<tr>
<td></td>
<td><strong>By Null String</strong></td>
</tr>
<tr>
<td></td>
<td>Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.</td>
</tr>
<tr>
<td></td>
<td><strong>By Existing Certificate (Precedence to LSC)</strong></td>
</tr>
<tr>
<td></td>
<td>Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the UDT. If a LSC exists in the UDT, authentication occurs via the LSC, regardless of whether a MIC exists in the UDT. If a MIC and LSC exist in the UDT, authentication occurs via the LSC. If a LSC does not exist in the UDT, but a MIC does exist, authentication occurs via the MIC.</td>
</tr>
<tr>
<td></td>
<td>At any time, the UDT uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the UDT at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode.</td>
</tr>
<tr>
<td></td>
<td><strong>By Existing Certificate (Precedence to MIC)</strong></td>
</tr>
<tr>
<td></td>
<td>Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the UDT. If a MIC exists in the UDT, authentication occurs via the MIC, regardless of whether a LSC exists in the UDT. If a LSC exists in the UDT, but a MIC does not exist, authentication occurs via the LSC.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication String</td>
<td>If you select the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or select the <strong>Generate String</strong> button to generate a string. <strong>Note</strong> Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, a user or administrator must enter the authentication string on a device.</td>
</tr>
<tr>
<td>Key Size (Bits)</td>
<td>For this setting that is used for CAPF, select the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. <strong>Note</strong> If you select a higher key size than the default setting, the UDT takes longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the UDT to function while the action occurs. Key generation takes up to 30 or more minutes to complete. <strong>Note</strong> The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.</td>
</tr>
</tbody>
</table>

### Service Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Enter the location (URL) of the help text for the information button. Leave this field blank to accept the default setting.</td>
</tr>
<tr>
<td>Directory</td>
<td>Enter the server from which the UDT obtains directory information. Leave this field blank to accept the default setting.</td>
</tr>
<tr>
<td>Messages</td>
<td>Leave this field blank (not used by Unified CM).</td>
</tr>
<tr>
<td>Services</td>
<td>Enter the location (URL) for IP phone services.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>Enter the URL that the UDT uses to validate requests that are made to the web server. If you do not provide an authentication URL, the advanced features for UDT that require authentication do not function. By default, this URL accesses a Unified CM User Options window that was configured during installation. Leave this field blank to accept the default setting.</td>
</tr>
</tbody>
</table>
### Universal Device Template setup

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Proxy Server           | Enter the host and port (for example, proxy.cisco.com:80) that are used to proxy HTTP requests for access to non-local host addresses from the HTTP client.  

The rule contains two parts for when to use the proxy server parameter:

- The hostname contains a "."  
- The hostname specifies an IP address in any form.  

If you do not configure this URL, the UDT attempts to connect directly to the URL.  
To accept the default setting, leave this field blank. |
| Idle                   | Enter the URL that appears on the display when the UDT device is not used for the time that is specified in Idle Timer field. For example, you can display a logo on the LCD when the UDT device is not used for 5 minutes.  

To accept the default setting, leave this field blank. |
| Idle Timer (seconds)   | Enter the time (in seconds) that you want to elapse before the URL that is specified in the Idle field appears.  

To accept the value of the Idle URL Timer enterprise parameter, leave this field blank. |
| Secure Authentication URL | Enter the secure URL that the UDT device uses to validate requests that are made to the web server.  

**Note** If you do not provide a Secure Authentication URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities.  
By default, this URL accesses a Unified CM User Options window that was configured during installation.  
Leave this field blank to accept the default setting.  
Maximum length: 255 |
| Secure Directory URL   | Enter the secure URL for the server from which the UDT obtains directory information. This parameter specifies the URL that this UDT uses when you press the Directory button.  

**Note** If you do not provide a Secure Directory URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities.  
Leave this field blank to accept the default setting.  
Maximum length: 255 |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Idle URL</td>
<td>Enter the secure URL for the information that appears on the display when this UDT is idle, as specified in Idle Timer field. For example, you can display a logo on the LCD when the UDT is not used for 5 minutes.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not provide a Secure Idle URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities.</td>
</tr>
<tr>
<td></td>
<td>To accept the default setting, leave this field blank.</td>
</tr>
<tr>
<td></td>
<td>Maximum length: 255</td>
</tr>
<tr>
<td>Secure Information URL</td>
<td>Enter the secure URL for the server location where the UDT can find help text information. This information appears when the user presses the information (I) button or the question mark (?) button.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not provide a Secure Information URL, this UDT uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, this UDT selects the appropriate URL, based on its capabilities.</td>
</tr>
<tr>
<td></td>
<td>To accept the default setting, leave this field blank.</td>
</tr>
<tr>
<td></td>
<td>Maximum length: 255</td>
</tr>
<tr>
<td>Secure Messages URL</td>
<td>Enter the secure URL for the messages server. This UDT contacts this URL when the user presses the Messages button.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not provide a Secure Messages URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities.</td>
</tr>
<tr>
<td></td>
<td>To accept the default setting, leave this field blank.</td>
</tr>
<tr>
<td></td>
<td>Maximum length: 255</td>
</tr>
<tr>
<td>Secure Services URL</td>
<td>Enter the secure URL for Cisco Unified IP Phone services. The Secure Services URL is the location that the UDT contacts when the user presses the Services button.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not provide a Secure Services URL, a device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, a device chooses the appropriate URL, based on its capabilities.</td>
</tr>
<tr>
<td></td>
<td>To accept the default setting, leave this field blank.</td>
</tr>
<tr>
<td></td>
<td>Maximum length: 255</td>
</tr>
</tbody>
</table>
From the drop-down list box, select how the UDT supports the services:

**Internal**

The UDT uses the phone configuration file to support the service.

Select this option or Both for Cisco-provided default services where the Service URL was not updated; that is, the service URL indicates Application:Cisco/<name of service>; for example, Application:Cisco/CorporateDirectory.

Select Internal or Both for Cisco-signed Java MIDlets because Cisco-signed Java MIDlets are provisioned in the configuration file.

**External URL**

Selecting External URL indicates that the UDT ignores the services in the phone configuration file and retrieves the services from a Service URL.

If you configure a custom Service URL for a service, including a Cisco-provided default service, you must choose either External URL or Both; if you choose Internal in this case, the services that are associated with the custom URLs do not work on the UDT.

**Both**

Selecting Both indicates that the UDT supports both the services that are defined in the configuration file and external applications that are retrieved from service URLs.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Capture Mode</td>
<td>This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box:</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong></td>
</tr>
<tr>
<td></td>
<td>This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Batch Processing Mode</strong></td>
</tr>
<tr>
<td></td>
<td>Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. The system creates a new file daily with a new encryption key. Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.</td>
</tr>
<tr>
<td></td>
<td>For more information about packet capturing, see the <em>Troubleshooting Guide for Cisco Unified Communications Manager</em>.</td>
</tr>
<tr>
<td>Packet Capture Duration</td>
<td>This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, appears.</td>
</tr>
<tr>
<td></td>
<td>For more information about packet capturing, see the <em>Cisco Unified Communications Manager Troubleshooting Guide</em>.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Secure Shell User | Enter a user ID for the secure shell user. You can enter any alphanumeric or special characters up to 50 characters. Invalid characters include ", %, &<,>, and \. This field appears when the UDT supports SSH access.
Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance.
For more information about how to configure encrypted phone configuration files to ensure that the Unified CM does not send unencrypted SSH credentials to the UDT device, see the *Cisco Unified Communications Manager Security Guide*.

Secure Shell Password | Enter the password for a secure shell user. You can enter any alphanumeric or special characters up to 200 characters. Invalid characters include ", %, &<,>, and\. Contact TAC for further assistance.
For more information about configuring encrypted phone files to ensure that Unified CM does not send unencrypted SSH passwords to the UDT device, see the *Cisco Unified Communications Manager Security Guide*.

### Locale Settings

**User Locale** | From the drop-down list box, select the locale that is associated with the UDT. The user locale identifies a set of detailed information to support users, including language and font.
*Note* | If no user locale is specified, Unified CM uses the user locale that is associated with the device pool.
*Note* | If the users require that information appear in any language other than English, verify that the locale installer is installed before you configure the user locale. See the Unified CM Locale Installer documentation.

**Network Locale** | From the drop-down list box, select the locale that is associated with the UDT. The network locale contains a definition of the tones and cadences that the UDT in a specific geographic area uses.
*Note* | If no network locale is specified, Unified CM uses the network locale that is associated with the device pool.
*Note* | If users require that country-specific tones be played, verify that the locale is installed before you configure the network locale. See the Unified CM Locale Installer documentation.

### Multilevel Precedence Preemption (MLPP) Settings
Select an MLPP domain from the drop-down list box for the MLPP domain that is associated with this UDT. If you leave the None value, devices with this UDT inherit the MLPP domain from the value that was set for the device pool. If the device pool does not have an MLPP domain setting, this UDT inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.

If available, this setting specifies whether a device that can play precedence tones uses the capability when it places an MLPP precedence call.

From the drop-down list box, select a setting to assign to this UDT from the following options:

- **Default**: This UDT inherits its MLPP indication setting from its device pool.
- **Off**: This UDT does not handle nor process indication of an MLPP precedence call.
- **On**: This UDT does handle and process indication of an MLPP precedence call.

Do not configure a UDT with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the UDT.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Domain</td>
<td>Select an MLPP domain from the drop-down list box for the MLPP domain that is associated with this UDT. If you leave the None value, devices with this UDT inherit the MLPP domain from the value that was set for the device pool. If the device pool does not have an MLPP domain setting, this UDT inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
<tr>
<td>MLPP Indication</td>
<td>If available, this setting specifies whether a device that can play precedence tones uses the capability when it places an MLPP precedence call. From the drop-down list box, select a setting to assign to this UDT from the following options: Default: This UDT inherits its MLPP indication setting from its device pool. Off: This UDT does not handle nor process indication of an MLPP precedence call. On: This UDT does handle and process indication of an MLPP precedence call. Note: Do not configure a UDT with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful. Note: Turning on MLPP Indication (at the enterprise parameter, device pool, or device level) disables normal Ring Setting behavior for the lines on a device, unless MLPP Indication is turned off (overridden) for the UDT.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MLPP Preemption</td>
<td>If available, this setting specifies whether this UDT that can preempt calls in progress uses the capability when it places an MLPP precedence call. From the drop-down list box, select a setting to assign to this UDT from the following options:</td>
</tr>
</tbody>
</table>
|                       | **Default**  
|                       | This UDT inherits its MLPP preemption setting from its device pool.                                                                                                                                             |
|                       | **Disabled**  
|                       | This UDT does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.                                                                        |
|                       | **Forceful**  
|                       | This UDT allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls.                                                                              |
|                       | **Note**      
|                       | Do not configure a UDT with the following combination of settings: MLPP Indication is set to **Off** or **Default** (when default is **Off**) while MLPP Preemption is set to **Forceful**.  |

### Do Not Disturb (DND) Settings

| Do Not Disturb | Check this check box to enable Do Not Disturb (DND) for this UDT. |
When you enable DND on the UDT, this parameter allows you to specify how the DND features handle incoming calls:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DND Option</strong></td>
<td>When you enable DND on the UDT, this parameter allows you to specify how the DND features handle incoming calls:</td>
</tr>
<tr>
<td><strong>Call Reject</strong></td>
<td>This option specifies that no incoming call information is presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the UDT may play a beep or display a flash notification of the call.</td>
</tr>
<tr>
<td><strong>Ringer Off</strong></td>
<td>This option turns off the ringer, but incoming call information gets presented to the UDT, so the user can accept the call.</td>
</tr>
<tr>
<td><strong>Use Common Phone Profile Setting</strong></td>
<td>This option specifies that the device on the UDT uses the DND Option setting from the Common Phone Profile window.</td>
</tr>
</tbody>
</table>

**Note** For 7940 and 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 is presented to the device.
When you enable the DNDRinger Off or Call Reject option, this parameter specifies how a call appears on a device. From the drop-down list, select one of the following options:

**None**

This option specifies that this UDT uses the DND Incoming Call Alert setting from the Common Phone Profile window.

**Disable**

This option disables both beep and flash notification of a call, but, for the DNDRinger Off option, incoming call information still appears. For the DNDCall Reject option, no call alerts appear, and no information is sent to the UDT.

**Beep Only**

For an incoming call, this option causes the associated device to play a beep tone only.

**Flash Only**

For an incoming call, this option causes the associated device to display a flash alert.

### Automatic Alternate Routing (AAR) Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR Group</td>
<td>Select the automated alternate routing (AAR) group for this UDT. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. If no AAR group is specified, Unified CM uses the AAR group that is associated with Device Pool or Line.</td>
</tr>
<tr>
<td>AAR Calling Search Space</td>
<td>Select the appropriate calling search space for this UDT to use when it performs automated alternate routing (AAR). The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth.</td>
</tr>
</tbody>
</table>

### Busy Lamp Field Settings
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLF Presence Group</td>
<td>Configure this field with the BLF Presence feature. From the drop-down list box, select a BLF presence group for this UDT. The selected group specifies the devices, end users, and application users that can monitor this directory number. The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF presence groups that are configured in Unified CM Administration also appear in the drop-down list box. Presence authorization works with BLF presence groups to allow or block presence requests between groups. For more information about how to configure permissions between groups and how presence works with Cisco Extension Mobility, see the “BLF Presence” chapter in the <em>Cisco Unified Communications Manager Features and Services Guide</em>.</td>
</tr>
</tbody>
</table>
| BLF Audible Alert Setting (Phone Idle) | This setting determines the busy lamp field (BLF) audible alert setting when no current call exists on the BLF DN:  
  **On**  
  An audible alert sounds.  
  **Off**  
  No audible alert sounds.  
  **Default**  
  The configuration in the Service Parameters Configuration window determines the alert option.                                                                                                                                                        |
| BLF Audible Alert Setting (Phone Busy) | This setting determines the BLF audible alert setting when at least one active call exists on the BLF DN, but no call pickup alerts exist:  
  **On**  
  An audible alert sounds.  
  **Off**  
  No audible alert sounds.  
  **Default**  
  The configuration in the Service Parameters Configuration window determines the alert option.                                                                                                                                                        |

**Music on Hold Settings**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| User Hold MOH Audio Source                 | To specify the audio source that plays when a user initiates a hold action, select an audio source from the drop-down list box. If you do not select an audio source, Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID.  
**Note**: You define audio sources in the Music On Hold Audio Source Configuration window. For access, select Media Resources > Music on Hold Audio Source.                                                                                       |
| Network Hold MOH Audio Source              | To specify the audio source that plays when the network initiates a hold action, select an audio source from the drop-down list box. If you do not choose an audio source, Unified CM uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID.  
**Note**: You define audio sources in the Music On Hold Audio Source Configuration window. For access, select Media Resources > Music on Hold Audio Source.                                                                                       |
| **Location Settings**                       |                                                                                                                                                                                                                                                                                                                                                                                                   |
| 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, select the appropriate location for this UDT.  
A location setting of **Hub_None** means that the locations feature does not keep track of bandwidth. A location setting of **Phantom** specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.  
To configure a new location, use the **System > Location Info > Location** menu option.  
For more information about location-based CAC across intercluster trunks, see “Location-Based Call Admission Control Over Intercluster Trunk” in the Cisco Unified Communications Manager System Guide.                                                                                       |
| Geolocation                                | From the drop-down list box, select a geolocation.  
You can select the **Unspecified** geolocation, which designates that this UDT does not associate with a geolocation. 
You can also select a geolocation that is configured with the **System > Geolocation Configuration** menu option.                                                                                                                                                                                                                       |
From the drop-down list box, turn the device mobility mode on or off for this UDT or select Default to use the default device mobility mode. The default setting uses the value for the Device Mobility Mode service parameter.

Click View Current Device Mobility Settings to display the current values of these device mobility parameters:

- Cisco Unified Communications Manager Group
- Roaming Device Pool
- Location
- Region
- Network Locale
- AAR Group
- AAR Calling Search Space
- Device Calling Search Space
- Media Resource Group List
- SRST

For more information, see “Device Mobility” in the Cisco Unified Communications Manager Features and Services Guide.

Select the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List.

If you choose None, Unified CM uses the Media Resource Group List that is defined in the device pool.

For more information, see the “Media Resource Management” section in the Cisco Unified Communications Manager System Guide.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Mobility Mode</td>
<td>From the drop-down list box, turn the device mobility mode on or off for this UDT or select Default to use the default device mobility mode. The default setting uses the value for the Device Mobility Mode service parameter. Click View Current Device Mobility Settings to display the current values of these device mobility parameters: Cisco Unified Communications Manager Group, Roaming Device Pool, Location, Region, Network Locale, AAR Group, AAR Calling Search Space, Device Calling Search Space, Media Resource Group List, SRST. For more information, see “Device Mobility” in the Cisco Unified Communications Manager Features and Services Guide.</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>Select the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List. If you choose None, Unified CM uses the Media Resource Group List that is defined in the device pool. For more information, see the “Media Resource Management” section in the Cisco Unified Communications Manager System Guide.</td>
</tr>
</tbody>
</table>
If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device check box. Checking this check box tells Unified CM to allocate a buffer for the UDT when it registers and to bundle SCCP messages.

**Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays for phones that are running SCCP. Most users do not require this option. Unified CM sends the bundled messages to the UDT when the station buffer is full, as soon as it receives a media-related message, or when the Bundle Outbound SCCP Messages timer expires.

**Note** To specify a setting other than the default setting (100 msec) for the Bundle Outbound SCCP Messages timer, set up a new value in the Service Parameters Configuration window for the Cisco CallManager service. Although 100 msec specifies the recommended setting, you may enter 15 msec to 500 msec.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Device</td>
<td>If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device check box. Checking this check box tells Unified CM to allocate a buffer for the UDT when it registers and to bundle SCCP messages.</td>
</tr>
</tbody>
</table>
Feature group template setup

This chapter contains information to set up feature group templates.

- Feature group template setup, page 857

Feature group template setup

In Cisco Unified Communications Manager (Unified CM) Administration, use the User Management > User/Phone Add > Feature Group Templates menu path to set up a feature template that includes features such as mobility and IM and Presence. You can also assign a pre-configured service profile and universal device templates to a user.

Note

You set up feature group templates that you use when you add a user or device from the Quick User/Phone Add window. Changes to the template do not affect users and devices that are already added.

This table lists and describes the field settings on the Feature Group template window.

Table 125: Feature group template settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Group Templates</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the feature group template identification name.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the feature group template. The description can be up to 100 characters in any language, and most punctuation is allowed.</td>
</tr>
<tr>
<td>Features</td>
<td></td>
</tr>
<tr>
<td>Home Cluster</td>
<td>Check this check box if the end user is homed to this cluster. The end user should only be homed to one cluster within the enterprise.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> IM and Presence does not function properly if an end user is assigned to more than one cluster.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile) | Check this check box to enable the end user (on the home cluster) for IM and Presence. Configure IM and Presence in the associated service profile.  
**Note** You must install a Cisco Unified Communications Manager IM and Presence Service node along with Cisco Unified Communications Manager.  
Use the **User Management > User Settings > UC Services** menu to configure the settings for the IM and Presence Service. |
| Service Profile                                            | Select a service profile from the drop-down list box. To view the settings for each service profile, select the **More Details** link.  
**Note** You can create new service profiles from the **User Management > User Settings > Service Profile** menu. |
| Allow Control of Device from CTI                          | If you check this check box, the AllowCTIControlFlag device property becomes active, which allows control of the device from computer telephony integration (CTI) applications. This setting takes effect when the user signs in to a device or the device is in the user CTI control device list.  
**Note** If the user does not sign into a device or no device exists in the user CTI control device list, this setting has no effect.  
The Allow Control of Device from CTI setting in the end user configuration overrides the AllowCTIControlFlag device property of the device to which the user signs in. |
| Enable Extension Mobility Cross Cluster                    | Check this check box to enable this end user to use the Cisco Extension Mobility Cross Cluster feature.                                                                                                     |
| Enable Mobility                                            | Check this check box to activate Mobile Connect, which allows the user to manage calls through a single phone number and to pick up in-progress calls on the desk phone and mobile phone.                                      |
| Enable Mobile Voice Access                                 | Check this check box to allow the user to access the Mobile Voice Access integrated voice response (IVR) system to initiate Mobile Connect calls and activate or deactivate Mobile Connect capabilities.                                |
| Maximum Wait Time for Desk Pickup *                       | Enter the maximum time in milliseconds that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to desktop phone.  
Default: 10000                                                                                                     |
| Remote Destination Limit *                                 | Enter the maximum number of phones to which the user is permitted to transfer calls from the desktop phone.  
Default: 4                                                                                                           |
### Field | Description
--- | ---
BLF Presence Group * | Use this field to configure the BLF Presence feature.  
From the drop-down list box, choose a BLF presence group for the end user. The selected group specifies the destinations that the end user can monitor.  
The default value for BLF Presence Group specifies Standard Presence group, configured with installation. BLF presence groups that are configured in Cisco Unified CM Administration also appear in the drop-down list box.  
BLF presence authorization works with BLF presence groups to allow or block presence requests between groups. For more information about how to configure permissions between groups and how BLF presence works with extension mobility, see the *Cisco Unified Communications Manager Features and Services Guide*.  

SUBSCRIBE Calling Search | Supported with the BLF presence feature, the SUBSCRIBE calling search space determines how Unified CM routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user.  
From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Unified CM Administration appear in the SUBSCRIBE Calling Search Space drop-down list box.  
If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None.  
To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.  

User Locale | From the drop-down list box, choose the locale that is associated with the end user. The user locale identifies a set of detailed information to support end users, which includes language and font.  
Unified CM uses this locale for extension mobility and the Unified CM User Options. For Cisco Extension Mobility login, the locale that is specified here takes precedence over the device and device profile settings. For Cisco Extension Mobility logout, Cisco Unified CM uses the end user locale that the default device profile specifies.  
*Note* If you do not choose an end user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.  

Universal Device Templates  
*Note* These templates are used to create new phones or move phones for the users associated with this feature group template.  

Mobile Phones | From the drop-down list box, select a universal device template for mobile devices that are associated to this user.
### Field | Description
--- | ---
Profiles | From the drop-down list box, select a universal device template for profiles that are associated to this user.
Quick user and phone addition

This chapter contains information to quickly add users and phones to Cisco Unified Communications Manager (Unified CM).

- Quick user and phone addition configuration and settings, page 861
- Add new user and device, page 863
- Add new user and existing device, page 864
- Move device to a user, page 865

Quick user and phone addition configuration and settings

In Cisco Unified Communications Manager (Unified CM) Administration, use the User Management > User/Phone Add > Quick User/Phone Add menu path to configure a user, a phone, and a line appearance in a single, easy addition.

The Quick User/Phone Add window in Unified CM provides a single window that allows you to perform basic steps to add a new user and assign the phones to the user.

Before you add a user and phone from this window, ensure that you have performed the following prerequisites:

- Set up a line (directory number)
- Set up a universal device template
- Set up a feature group template

Quick user and phone addition settings

The following table lists the quick user and phone addition settings.

Table 126: Quick user and phone addition settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Information</td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td>Enter the end user first name.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Middle Name</td>
<td>Enter the end user middle name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the end user last name.</td>
</tr>
<tr>
<td>User ID</td>
<td>Enter the end user identification name. Unified CM does not permit modifying the user ID after you create it.</td>
</tr>
</tbody>
</table>

#### Access Control Group Membership

User is a member of  
Select the plus sign (+) next to this drop-down list box to list the access control groups (ACGs). You can assign this user as an ACG member. ACGs allow users with full access to configure different levels of access for Unified CM administrators. Full-access users configure the access of other users to Unified CM.

**Tip**  
Select the plus sign (+) again to add more ACGs for the user.

#### Device Creation

Feature Group Template  
This drop-down list box lists the feature group templates to which you can assign this user. You can assign one template.

After you create the user and assign a feature group template, the **Manage Devices** button appears.

**Note**  
You have to add at least one extension before the **Manage Devices** button appears.

#### Credentials

Use default credential  
Use this setting to select the default credential, so you do not have to type credentials into a field. When you select this setting, the default credential defined in the system default credential policy is used automatically during the user insertion. The password and PIN input and confirm text box is disabled.

**Note**  
This setting is not supported for the update user operation.

Password  
Enter five or more alphanumeric or special characters for the user password. You may use the following special characters: `=, +, <, >, #, :, \, "`, and blank spaces.

Confirm Password  
Enter the user password again.

PIN  
Enter five or more numeric characters for the personal identification number (PIN).

Confirm PIN  
Enter the PIN again.
### Field Description

**Extension**
This field represents the extensions for the user. Extensions represent the lines that are added to a phone. These extensions are based on the available lines in the template. After you assign the first (primary) extension, the secondary extensions drop-down list box lists the available extensions.

To assist the administrator, the drop-down list box shows extensions as either "Available" or "Used."

**Note** You cannot add devices until you specify an extension.

**Note** You can add multiple extensions for the user. When you select the green plus sign (+) under Action, you can add more extensions and change their order of appearance.

**Personal**

**Directory URI**
Enter the directory uniform resource identifier (URI) for this user. A directory URI looks like an email address and follows the user@host format. It allows for others to find a user in a directory easily.

**Number Displayed in Directory**
Enter the user telephone number. This number shows up when you hit the company (local) directory button on your phone.

**Email**
Enter the user e-mail address.

**Manager User Id**
Enter the user ID of the manager.

**Note** The manager user ID that you enter does not have to exist in the same cluster as the user; therefore, Unified CM does not require that you enter a user ID that already exists in the database.

**Department**
Enter the user department information (for example, the department number or name).

### Related Topics

- Feature group template setup, on page 857
- Universal Device Template setup, on page 821

### Add new user and device

#### Procedure

**Step 1**
Select Add New.  
The Quick User/Phone Add window is displayed.

**Step 2**
Enter the appropriate settings.  
See topics related to quick user and phone addition for details.
Step 3 Select Save.
Step 4 Select Manage Devices.
Step 5 Select Add New Phone.
Step 6 Set the following fields:
   • Product Type
   • Device Protocol
   • Device Name
   • Universal Device Template
   • Is Extension Mobility Template
Step 7 Select Save.
The phone is added to the user.

Related Topics
Quick user and phone addition configuration and settings, on page 861

Add new user and existing device

Note Unified CM uses the three universal device templates that you defined on the Feature Group Template window to define the characteristics of devices.

Procedure

Step 1 Select Add New.
The Quick User/Phone Add window appears.
Step 2 Enter the appropriate settings as described in Quick user and phone addition configuration and settings, on page 861.
Step 3 Select Save.
The user is added to the Unified CM database.
Step 4 Select Manage Devices.
Step 5 Select Find a Phone to Move to This User.
Step 6 Select the phone you want to associate to the user.
   Note You can set search filters on the phone listing.
Step 7 Select Move Selected.
The phone is added to the user.
**Move device to a user**

*Note*  Be aware that when a device is moved to the user, that device is disassociated from the previous user.

**Procedure**

**Step 1**  In Unified CM Administration, select *User Management > User/Phone Add > Quick User/Phone Add*
The Find and List window appears. Records from an active (prior) query may also appear in the window.

**Step 2**  From the first drop-down list box, select a search parameter.

*Example:*  
Select *First Name* to search by the user first name.

**Step 3**  From the second drop-down list box, select a search pattern.

**Step 4**  Specify the appropriate search text, if applicable.

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

**Step 5**  Select *Find*.

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

**Step 6**  Select the user to which you wish to move an existing device. The user profile appears.

**Step 7**  Select the *Manage Devices* button.

**Step 8**  Select the *Find a Phone to Move to This User* button.

**Step 9**  Select the phone you want to associate to the user.

*Note*  
You can set search filters on the phone listing.

**Step 10**  Select *Move Selected*.
The phone is added to the user profile.

**Related Topics**

Quick user and phone addition configuration and settings, on page 861
Move device to a user
Other user management menu options

This chapter provides brief descriptions of selected User Management menu options that other documents describe in greater detail. A pointer to the document that contains more details is provided for each User Management menu option.
Cisco Unified Communications Manager Bulk Administration

- Bulk Administration Tool (BAT), page 871
Bulk Administration Tool (BAT)

In Cisco Unified Communications Manager Administration, use the Bulk Administration menu and the submenu options to configure entities in Cisco Unified Communications Manager through use of the Bulk Administration Tool.

The Cisco Unified Communications Manager Bulk Administration Tool (BAT), a web-based application, performs bulk transactions to the Cisco Unified Communications Manager database. BAT lets you add, update, or delete a large number of similar phones, users, or ports at the same time. When you use Cisco Unified Communications Manager Administration, each database transaction requires an individual manual operation, while BAT automates the process and achieves faster add, update, and delete operations.

You can use BAT to work with the following types of devices and records:

- Add, update, and delete Cisco Unified IP Phones including voice gateway (VGC) phones, computer telephony interface (CTI) ports, and H.323 clients
- Add, update, and delete users
- Add, update, and delete User Device Profiles
- Add, update, and delete Cisco Unified Communications Manager Assistant managers and assistants
- Add, update, and delete ports on a Cisco Catalyst 6000 FXS Analog Interface Module
- Add or delete Cisco VG200 and Cisco VG224 analog gateways and ports
- Add or delete Forced Authorization Codes
- Add or delete Client Matter Codes
- Add or delete Call Pickup Groups
- Update or export CUP/CUPC users
- Populate or depopulate the Region Matrix
- Insert, delete, or export the Access List
- Export or import configuration
- Insert, delete, or export Remote Destination and Remote Destination Profile

You can also work with these devices in combination with the user information. For example, when you add CTI ports and users, BAT allows you to “Enable CTI Application Use.” This saves time when you are adding users who have applications that require a CTI port, such as Cisco IP Softphone.
An optional component of BAT, the Cisco Unified Communications Manager Auto-Register Phone Tool (TAPS), further reduces the manual labor that is involved in administering a large system. When you need to add a large block of new phones, you can use BAT to add the devices with dummy media access control (MAC) addresses instead of entering each MAC address in the data input file. After the phones are installed, the phone users or the administrator can call the TAPS directory number, follow the voice prompts, and download the correct user device profiles for their phones.
Dependency records

This appendix provides information about the dependency record windows in Cisco Unified Communications Manager Administration. These windows help you to determine which records in the database use other records. For example, you can determine which devices (such as CTI route points or phones) use a particular calling search space.

If you need to delete a record from Cisco Unified Communications Manager, you can use dependency records to show which records are associated with the record that you want to delete. You can then reconfigure those records, so they are associated with a different record.

- Enable dependency records, page 873
- Disable dependency records, page 874
- Access dependency records, page 874
- Dependency record buttons, page 876

Enable dependency records

To access dependency records, you must first enable them. The system disables dependency records by default. To enable the dependency records, perform the following procedure.

Caution

Enabling the dependency records functionality causes high CPU usage. This task executes at below-normal priority and may take time to complete due to dial plan size and complexity, CPU speed, and the CPU requirements of other applications.

Procedure

Step 1  Choose System > Enterprise Parameters
Step 2  Scroll to the CCMAdmin Parameters area of the window.
Step 3  From the Enable Dependency Records drop-down list box, choose True. A dialog box displays with a message about the consequences of enabling the dependency records. Read the information carefully before clicking OK.
**Disable dependency records**

If you have dependency records enabled and your system is experiencing CPU usage issues, you can disable dependency records. (The system disables dependency records by default.) To disable the dependency records, perform the following procedure.

**Procedure**

1. Choose **System > Enterprise Parameters**.
2. Scroll to the CCMAdmin Parameters area of the window.
3. From the Enable Dependency Records drop-down list box, choose False. A dialog box displays with a message about dependency records. Read the information carefully before clicking OK.
4. Click OK. The field displays False.
5. Click Save.

**Access dependency records**

To access dependency records from Cisco Unified Communications Manager configuration windows, choose Dependency Records from the Related Links box and click Go. The Dependency Records—Summary window displays. This window displays the number and type of records that use the record that is shown in the Cisco Unified Communications Manager configuration window.

**Note**

If the dependency records are not enabled, the Dependency Records—Summary window displays a message, not the information about the record.
For example, if you display a the Default device pool in the Device Pool Configuration window and click the Dependency Records link, the Dependency Records Summary window displays all the records that use that device pool, as shown in the following figure.

*Figure 1: Dependency Records—Summary example*

To display detailed dependency records information, click the record about which you want more information; for example, click the trunk record. The Dependency Records Detail window displays, as shown in the following figure. If you want to return to the original configuration window, choose Back to Summary from
the Related List Box and click Go; then, choose Back to <configuration window name> and click Go, or click the Close and go Back button.

**Figure 2: Dependency Records—Detail example**

To display the configuration window of the record that is displayed in the Dependency Records Detail window, click the record. The configuration window for that record displays. For example, if you click the h225trunk record that is shown in the Dependency Record figure, the Trunk Configuration window displays with information about the h225trunk.

**Related Topics**

Enable dependency records, on page 873

---

**Dependency record buttons**

Three buttons display in the Dependency Records Summary window:

- **Refresh**—Updates the window with current information.
- **Close**—Closes the window but does not return to the Cisco Unified Communications Manager configuration window in which you clicked the Dependency Records link.
- **Close and Go Back**—Closes the window and returns to the Cisco Unified Communications Manager configuration window in which you clicked the Dependency Records link.
Non-Cisco SIP phones setup

This appendix provides information about Configuring Non-Cisco Phones That Are Running SIP.

- About non-Cisco SIP phone setup, page 877
- Third-party SIP phone setup process, page 877
- Different setups for SIP phones, page 879
- Where to find more information, page 882

About non-Cisco SIP phone setup

Cisco Unified Communications Manager supports Cisco Unified IP Phones with SIP as well as RFC3261-compliant phones that are running SIP from third-party companies. This appendix describes how to configure the third-party phones that are running SIP by using Cisco Unified Communications Manager Administration.

Third-party SIP phone setup process

Cisco Unified Communications Manager supports Cisco Unified IP Phones with SIP as well as RFC3261-compliant phones that are running SIP from third-party companies. You can manually configure a third-party phone that is running SIP by using Cisco Unified Communications Manager Administration.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Gather the information about the phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• MAC address</td>
</tr>
<tr>
<td></td>
<td>• Physical location of the phone</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager user to associate with the phone</td>
</tr>
<tr>
<td></td>
<td>• Partition, calling search space, and location information, if used</td>
</tr>
<tr>
<td></td>
<td>• Number of lines and associated DNs to assign to the phone</td>
</tr>
</tbody>
</table>
Step 2 Determine whether sufficient Device License Units are available. If not, purchase and install additional Device License Units. Third-Party SIP Devices (Basic) and (Advanced) consume three and six Device License Units each, respectively.
See topics related to calculating the number of required licenses and obtaining a license in the *Cisco Unified Communications Manager Features and Services Guide*.

Step 3 Configure the end user that will be the Digest User.
**Note** If the third-party phone that is running SIP does not support an authorization ID (digest user), create a user with a user ID that matches the DN of the third-party phone. For example, create an end user named 1000 and create a DN of 1000 for the phone. Assign this user to the phone (see Step 9, on page 878).

Step 4 Configure the SIP Profile or use the default profile. The SIP Profile gets added to the phone that is running SIP by using the Phone Configuration window.
**Note** Third-party phones that are running SIP use only the SIP Profile Information section of the SIP Profile Configuration window.

Step 5 Configure the Phone Security Profile. To use digest authentication, you must configure a new phone security profile. If you use one of the standard, nonsecure SIP profiles that are provided for auto-registration, you cannot enable digest authentication.

Step 6 Add and configure the third-party phone that is running SIP by choosing Third-party SIP Device (Advanced) or (Basic) from the Add a New Phone Configuration window.
**Note** Third-party SIP Device (Basic) supports one line and consumes three license units, and Third-party SIP Device (Advanced) supports up to eight lines and video and consumes six license units.

Step 7 Add and configure lines (DNs) on the phone.

Step 8 In the End User Configuration window, associate the third-party phone that is running SIP with the user by using Device Association and choosing the phone that is running SIP.

Step 9 In the Digest User field of the Phone Configuration window, choose the end user that you created in Step 3, on page 878.

Step 10 Provide power, install, verify network connectivity, and configure network settings for the third-party phone that is running SIP.
See the administration guide that was provided with your phone that is running SIP.

Step 11 Make calls with the third-party phone that is running SIP.
See the user guide that came with your third-party phone that is running SIP.

---

**Related Topics**
- Phone security profile setup, on page 147
- Directory number setup, on page 263
- Set up Cisco Unified IP Phone, on page 577
- Set up speed-dial buttons or abbreviated dialing, on page 582
- About SIP profile setup, on page 695
- About end user setup, on page 771
- Associate devices to end user, on page 785
- Enable digest authentication for third-party SIP phones, on page 880
Different setups for SIP phones

The following table provides a comparison overview of the configuration differences between Cisco Unified IP Phones and third-party phones that are running SIP.

Table 127: Model configuration comparison for phones that are running SIP

<table>
<thead>
<tr>
<th>Phone That Is Running SIP</th>
<th>Integrated with Centralized TFTP</th>
<th>Sends MAC Address</th>
<th>Downloads Softkey File</th>
<th>Downloads Dial Plan File</th>
<th>Supports Cisco Unified Communications Manager Failover and Fallback</th>
<th>Supports Reset and Restart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 7911, 7941, 7961, 7970, 7971</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7940, 7960</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7905, 7912</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Third-party phone that is running SIP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Use Cisco Unified Communications Manager Administration to configure third-party phones that are running SIP. The administrator must also perform configuration steps on the third-party phone that is running SIP; see following examples:

- Ensure proxy address in the phone is the IP or Fully Qualified Domain Name (FQDN) of Cisco Unified Communications Manager.
- Ensure directory number(s) in the phone match the directory number(s) that are configured for the device in Cisco Unified Communications Manager Administration.
- Ensure digest user ID (sometimes referred to as Authorization ID) in the phone matches the Digest User ID in Cisco Unified Communications Manager Administration.

Consult the documentation that came with the third-party phone that is running SIP for more information.

Related Topics
Where to find more information, on page 882
How Cisco Unified Communications Manager identifies third-party phones

Because third-party phones that are running SIP do not send a MAC address, they must identify themselves by using username.

The REGISTER message includes the following header:

Authorization: Digest username="swhite", realm="ccmsipline",
nonce="GBauADss2qoWr6k9y3hGGVDAqnLfoLk5", uri="sip:172.18.197.224", algorithm=MD5,
response="126c0643a4923359ab59d4f53494552e"

The username, swhite, must match an end user that is configured in the End User Configuration window of Cisco Unified Communications Manager Administration. The administrator configures the SIP third-party phone with the user; for example, swhite, in the Digest User field of Phone Configuration window.

Note

You can assign each end user ID to only one third-party phone (in the Digest User field of the Phone Configuration window). If the same end user ID is assigned as the Digest User for multiple phones, the third-party phones to which they are assigned will not successfully register.

Related Topics

Set up Cisco Unified IP Phone, on page 577
About end user setup, on page 771

Third-party phones running SIP and TFTP

Third-party phones that are running SIP do not get configured by using the Cisco Unified Communications Manager TFTP server. The customer configures them by using the native phone configuration mechanism (usually a web page or tftp file). The customer must keep the device and line configuration in the Cisco Unified Communications Manager database synchronized with the native phone configuration (for example, extension 1002 on the phone and 1002 in Cisco Unified Communications Manager). Additionally, if the directory number of a line is changed, ensure that it gets changed in both Cisco Unified Communications Manager Administration and in the native phone configuration mechanism.

Enable digest authentication for third-party SIP phones

To enable digest authentication for third-party phones that are running SIP, the administrator must create a Phone Security Profile. See the Cisco Unified Communications Manager Security Guide for details. On the Phone Security Profile Configuration window, check the Enable Digest Authentication check box. After the security profile is configured, the administrator must assign that security profile to the phone that is running SIP by using the Phone Configuration window. If this check box is not checked, Cisco Unified Communications Manager will use digest authentication for purposes of identifying the phone by the end user ID, and it will not verify the digest password. If the check box is checked, Cisco Unified Communications Manager will verify the password.
Cisco Unified Communications Manager does not support Transport Layer Security (TLS) from third-party phones that are running SIP.

**Related Topics**

Phone security profile setup, on page 147

**DTMF reception**

To require DTMF reception, check the Require DTMF Reception check box that displays on the Phone Configuration window in Cisco Unified Communications Manager Administration.

**Licensing third-party SIP phones**

Licensing of third-party phones that are running SIP enforces the following limitations:

- **Third-party SIP Device (Basic)**—Video calls do not get supported. Video enforcement occurs as part of the offer/answer process. If video-related media is provided as part of an offer or answer from a SIP device that is not permitted to negotiate video, only the non-video-related parts of the call get extended to the destination party. Similarly, a SIP endpoint that is not permitted to negotiate media will not receive any video-related media in the SDP that is sent from Cisco Unified Communications Manager.

- **Third-party SIP Device (Advanced) and (Basic)**—Cisco-specific SIP extensions do not get supported. Some Cisco-specific SIP extensions that are not supported include service URIs, header extensions, dialog subscriptions, and remote call control proprietary mime types. Cisco Unified Communications Manager will reject any request from a phone that is running SIP that is not permitted to use an advanced feature that uses a service request URI (such as Call Pickup URI, Meet Me Service URI). The SIP profile specifies service URIs. The profile gets assigned to SIP devices. Cisco Unified Communications Manager will block features that require the use of Cisco-specific SIP extensions.

Ensure that any wireless third-party SIP client or device is configured as a Third-Party SIP Device (Advanced) in conformance with Cisco Unified Communications Manager licensing policy.

For more information about Cisco SIP Extensions, contact your Cisco representative.

In Cisco Unified Communications Manager, Release 5.1(1) and above, certain characteristics for Basic and Advanced Third-Party phones that are running SIP changed. These characteristics include changes to the Maximum Number of Calls per Device, Default Maximum number of calls per DN, and Default Busy Trigger per DN fields that display on the Directory Number Configuration window in Cisco Unified Communications Manager Administration. The following tables provide more information.

**Table 128: Directory number migration changes for basic third-party phones that are running SIP**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Old Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Number of Calls Per Device</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>
For users that have third-party phones that are running SIP that are configured on any version of release 5.0 that are migrating/upgrading to release 6.0(1) or above, be aware that, after the upgrade, these devices retain their release 5.0 configured values. However, if users need to make changes to DN configuration values, users must change Maximum Number of Calls and Default Busy Trigger values on each DN.

For basic third-party phones that are running SIP, only one line value needs to be modified. However, for advanced third-party phones that are running SIP, users potentially must disassociate lines on the device before they can make any DN-related configuration changes. This situation potentially can happen if more than four lines are configured. An example scenario follows:

- Advanced phone configured with 6 lines with Maximum number of calls = 4 and Busy Trigger = 2 for each line.
- After upgrade to release 6.1, ensure maximum number of calls on the device is reduced to 16 or below before any DN changes. The current value on this phone equals 24 (6 lines * 4). The device essentially exists in a negative zone (16-24).
- User would disassociate two lines from the device.
- After the user disassociates those lines from the device, you can modify the DN characteristics for the remaining four lines by setting Maximum Number of Calls and Busy Trigger to an appropriate value.
- User reassociates the disassociated lines.

### Where to find more information

**Related Topics**

- Directory number setup, on page 263
- Cisco Unified IP Phone setup, on page 537
- SIP profile setup, on page 695
End user setup, on page 771
Third-party SIP phone setup process, on page 877
AS-SIP configuration

Assured Services SIP (AS-SIP) endpoints are SIP endpoints compliant with MLPP, DSCP, TLS/SRTP, and IPv6 requirements. AS-SIP provides for multiple endpoint interfaces on the Unified Communications Manager. The Third-Party AS-SIP Endpoint device type allows a third-party AS-SIP-compliant generic endpoint to be configured and used with the Unified CM.

The Cisco-proprietary RoundTable (RT) 8961, 9951 and 9971 SIP phones, and their corresponding Unified CM interfaces, are enhanced to provide AS-SIP features. The RT MLPP behavior maintains feature parity with SCCP MLPP implementation. The SIP signaling interface between Unified CM and RT phones is different from the interface between Unified CM and Third-Party AS-SIP Endpoint. The Unified CM sends new configuration parameters to the RT endpoint as part of the extended mark-up language (XML) configuration file. These parameters enable and disable the AS-SIP features and also govern how the RT endpoint operates when using this functionality. The RT endpoint also parses, processes, and sends new headers indicating resource priority for a given call. The RoundTable enhancements focus on TFTP configuration and SIP call processing exchanges between the RT endpoint and the Unified CM.

- AS-SIP capabilities, page 886
- Set up AS-SIP line endpoints, page 886
- Configuration differences for phones running AS-SIP, page 887
- AS-SIP conferencing, page 888
- Unified Communications Manager identification of third-party phones, page 889
- Third-party phones running AS-SIP, page 889
- End user configuration settings, page 889
- SIP profile configuration settings, page 890
- Require DTMF reception, page 891
- Set up phone security profile settings, page 891
- Set up TLS, page 891
- Add and configure third-party phones, page 891
AS-SIP capabilities

The following capabilities are implemented or made available for the Third-Party AS-SIP Endpoint interface in compliance with LSC and AS-SIP Line requirements:

- MLPP
- TLS
- SRTP
- DSCP for precedence levels
- Error responses
- V.150.1 MER
- Conference Factory flow support
- MLPP Authentication and Authorization
- AS-SIP Line Early Offer

Note

With the exception of AS-SIP Line Early Offer, these capabilities were also implemented, made available, or already existed for the RT 8961, 9951 and 9971 phones and corresponding Unified CM interfaces, in compliance with LSC and SIP EI requirements.

Set up AS-SIP line endpoints

Unified CM supports Cisco Unified IP Phones with SIP as well as RFC3261-compliant phones that are running SIP from third-party companies. This procedure lists the tasks used to manually configure a third-party phone that is running SIP. Use Cisco Unified Communications Manager Administration to configure third party phones.

Procedure

Step 1 Gather the following information about the phone:
- Physical location of the phone Unified Communications Manager user to associate with the phone
- Partition, calling search space, and location information, if used
- Number of lines and associated DNs to assign to the phone

Step 2 Determine whether sufficient Device License Units are available.
All licensing for Unified CM and Unity Connection is centralized and held on the Enterprise License Manager. For more information, refer to the Enterprise License Manager User Guide.

Step 3 Configure the end user that will be the Digest User.
See topics related to End User configuration settings for field descriptions.
MLPP authentication (optional) requires the phone to send an MLPP username and password. The end user specifies the highest MLPP precedence level allowed for that user. MLPP credentials are tied to the user while the need to use them is tied to the device (via the MLPP Authorization checkbox in the SIP Profile used by the device).

Step 4 Configure the SIP Profile or use the default profile. The SIP Profile gets added to the phone that is running SIP by using the Phone Configuration window.
Third-party AS-SIP phones use the SIP Profile Information section of the SIP Configuration window along with the following fields from the phone specific parameters section:

- Resource Priority Namespace
- MLPP User Authorization

Note The phone specific parameters are not downloaded to a third-party AS-SIP phone. They are only used by the Unified CM. Third party phones must locally configure the same settings. See topics related to SIP profile configuration settings and configuring Cisco Unified IP Phones for more information.

Step 5 Configure the phone security profile.
To use digest authentication, you must configure a new phone security profile. If you use one of the standard, nonsecure SIP profiles that are provided for auto-registration, you cannot enable digest authentication. See topics related to phone security profile configuration and the Cisco Unified Communications Manager Security Guide for more information.

The phone security profile must be configured for TLS. See “TLS” section for details.

Step 6 Add and configure the third-party phone that is running SIP by choosing Third-party AS-SIP Endpoint from the Add a New Phone Configuration window.
See topics related to configuring Cisco Unified IP Phones for more information.

Step 7 Add and configure lines (DNs) on the phone.
See topics related to directory number configuration for more information.

Step 8 In the End User Configuration window, associate the third-party phone that is running SIP with the user by using Device Association and choosing the phone that is running SIP.
See topics related to associating devices to an end user for more information.

Step 9 In the Digest User field of the Phone Configuration window, choose the end user that you created in Step 3.

Step 10 Provide power, install, verify network connectivity, and configure network settings for the third-party phone that is running SIP.
See the administration guide that was provided with your phone that is running SIP.

Step 11 Make calls with the third-party phone that is running AS-SIP.
See the user guide that came with your third-party phone that is running SIP.

Configuration differences for phones running AS-SIP

The following table provides a comparison overview of the configuration differences between Cisco Unified IP Phones and third-party phones that are running AS-SIP.
Use Unified CM Administration to configure third-party phones that are running SIP (see the “SIP Profile Configuration Settings” section). The administrator must also perform configuration steps on the third-party phone that is running SIP; see following examples:

- Ensure proxy address in the phone is the IP or Fully Qualified Domain Name (FQDN) of Unified Communications Manager.
- Ensure directory number(s) in the phone match the directory number(s) that are configured for the device in Unified CM Administration.
- Ensure digest user ID (sometimes referred to as Authorization ID) in the phone matches the Digest User ID in Unified CM Administration.

Consult the documentation that came with the third-party phone that is running SIP for more information.

**AS-SIP conferencing**

MOH is applied to its target (a held party, transferee just prior to transfer, or conferee just prior to joining the conference), if the feature invoker (holder, transferor, or conference initiator) supports Cisco-proprietary feature signaling. If the feature invoker does not support Cisco-proprietary feature signaling then MOH is not applied to its target. Also, if an endpoint explicitly signals that it is a conference mixer, then MOH will not be played to the target. There are two forms of AS-SIP Conferencing:

- Local mixing
- Conference factory

**Local mixing**

To the Unified CM, the conference initiator simply appears to have established simultaneously active calls, one to each of the other conference attendees. The conference is hosted locally by the initiator and the voices are mixed there. The calls from the conference initiator have special signaling that prevent it from being connected to an MOH source.

**Conference factory**
The conference initiator calls a Conference Factory Server located off of a SIP trunk. Through IVR signaling, the conference initiator instructs the Conference Factory to reserve a conference bridge. The Conference Factory gives the numeric address (a routable DN) to the conference initiator, who then establishes a subscription with the bridge to receive conference list information to keep track of participants. The Conference factory sends special signaling that will prevent it from being connected to an MOH Source.

**Unified Communications Manager identification of third-party phones**

Because third-party phones that are running SIP do not send a MAC address, they must identify themselves by using username.

The REGISTER message includes the following header:

Authorization: Digest

username="swhite",realm="ccmsipline",nonce="GBauADss2qpWr6k9y3hGGVDAgnLfoLk5",uri ="sip:172.18.197.224",algorithm=MD5,response="126c0643a4923359ab59d4f53494552c"

The username, swhite, must match an end user that is configured in the End User Configuration window of Unified CM Administration (see End User Configuration Settings). The administrator configures the SIP third-party phone with the user, for example, swhite, in the Digest User field of Phone Configuration window (see Configuring Cisco Unified IP Phones).

---

**Note**

You can assign each end user ID to only one third-party phone (in the Digest User field of the Phone Configuration window). If the same end user ID is assigned as the Digest User for multiple phones, the third-party phones to which they are assigned will not successfully register.

**Third-party phones running AS-SIP**

Third-party phones that are running AS-SIP do not get configured by using the Unified Communications Manager TFTP server. The customer configures them by using the native phone configuration mechanism (usually a web page or tftp file). The customer must keep the device and line configuration in the Unified Communications Manager database synchronized with the native phone configuration (for example, extension 1002 on the phone and 1002 in Unified Communications Manager). Additionally, if the directory number of a line is changed, ensure that it gets changed in both Unified CM Administration and in the native phone configuration mechanism.

**End user configuration settings**

The End User Configuration window in Unified CM Administration allows the administrator to add, search, display, and maintain information about Unified Communications Manager end users. End users can control phones after you associate a phone in the End User Configuration window. If MLPP Authorization is enabled for AS-SIP, MLPP Authorization must also be configured on the End User administration page. This MLPP Authentication requires a user identification number and a password. The MLPP User Identification number must be composed of 6 - 20 numeric characters and the MLPP Password must be composed of 4 - 20 numeric
characters. The Precedence Authorization level can be set to any standard precedence level from Routine to Executive Override.

Note
Extension Mobility is not supported for third-party AS-SIP devices.

Note
Third-party AS-SIP does not support CAPF.

SIP profile configuration settings

The SIP profile configuration settings contains an 'Is Assured SIP Service Enabled' checkbox. This should be checked for third-party AS-SIP endpoints, as well as AS-SIP trunks. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.

Enable digest authentication for third-party phones running SIP

To enable digest authentication for third-party phones that are running SIP, the administrator must create a Phone Security Profile. (See the "Phone Security Profile Configuration" section a general description and the Unified Communications Manager Security Guide for details.) On the Phone Security Profile Configuration window, check the Enable Digest Authentication check box. After the security profile is configured, the administrator must assign that security profile to the phone that is running SIP by using the Phone Configuration window. If this check box is not checked, Unified CM will use digest authentication for purposes of identifying the phone by the end user ID, and it will not verify the digest password. If the check box is checked, Unified CM will verify the password.

DTMF Reception

To require DTMF reception, check the Require DTMF Reception check box that displays on the Phone Configuration window in Unified CM Administration.

Phone Security Profile Configuration

In Unified CM Administration, use the System > Security > Phone Security Profile menu path to configure phone security profiles.

The Phone Security Profile window includes security-related settings such as device security mode, CAPF settings, digest authentication settings (only for phones that are running SIP), and encrypted configuration file settings. You must apply a security profile to all phones that are configured in Unified CM Administration.
Require DTMF reception

Set up phone security profile settings

Set up TLS

For TLS for third-party AS-SIP devices, configure your call manager correctly using the procedures found in the Security chapter in the Unified Communications Operating System Administration Guide.

You will also need to follow your local procedures for generating certificates.

For information on configuring and applying a phone security profile, see the Unified Communications Manager Security Guide.

Add and configure third-party phones

Adding and configuring AS-SIP devices is virtually identical to existing third-party device types. There are, however, a few differences. The AS-SIP device type:

- Can be configured for MLPP
- Includes an optional Device Security Mode in the security profile
- For Third-party AS-SIP devices, the preemption setting is not available on the Unified CM. It is completely controlled by the third-party phone.
- Supports Early Offer for voice and video calls

Note

Early Offer support for voice and video calls sends an SDP offer in the initial INVITE to the called party.

If Early Offer is enabled for a device, and the Unified CM expects to receive delayed offer calls, a Media Resource Group List must be configured in order to prevent the insertion of MTPs.

Use the following procedure to configure a media resource group list.

Procedure

Step 1
In CUCM Administration, choose Media Resources > Media Resource Group.

Step 2
Click the Add New button to add a new Media Resource Group List.

Step 3
In the Media Resource Group List, add only the Unified CM-based software MTPs to the Media Resource Group (MRG). Unified CM software resources are typically named MTP_# where # is a number (for example, "MTP_2").

Step 4
This media resource group, which should now contain all the software MTP resources from Unified CM, should not be applied to any media resource group list (MRGL). By placing the MTP resources in an MRG,
but not in an MRGL, these MTP resources are not be available to any of the devices on the system—which is the desired behavior.

**Note** If the system also has configured hardware MTP resources (which it does not by default), these must also be made unavailable using the same procedure.

For more information on adding and configuring third party phones, see Cisco Unified IP Phone Configuration, CUCM Administration Guide.
INDEX

A

AAR, See automated alternate routing (AAR)
abbreviated dial 570
configuration settings (table) 570
access control groups 791
described 791
related topics 791
access list 326
accessibility 21, 22
accessing buttons and icons 21, 22
adding records 17
Cisco Unified Communications Manager Administration 17
admission control 107
implementing with locations 107
analog access gateways and ports 532
adding 532
announcements 377
annunciator 333, 336
configuration overview 333
configuration settings (table) 333
related topics 333
synchronizing configuration 336
application dial rules 155, 157
configuration overview 155
configuration settings (table) 155
related topics 155
re prioritizing 157
application server 135
configuration 135
configuration settings (table) 135
related topics 135
application user 759, 765, 767, 768, 769
adding an administrator user to Cisco Unity or Cisco Unity Connection 765
associating devices to an application user 769
changing password 767
configuration 759
configuration settings (table) 759
credential settings (table) 768
managing credential information 767
related topics 759
automated alternate routing (AAR) 151
groups 151
configuration settings (table) 151
overview 151
related topics 151
autoregistration 139, 141, 143
configuration settings (table) 139
configuring 139
disabling 143
enabling 141
related topics 139
reusing autoregistration numbers 143

B

BAT 871
application overview 871
BLF presence groups 145
configuring 145
BLF/SpeedDial 576
configuration settings 576
BRI 502, 528
gateway configuration 502
ports, adding 528
browsers 4
browsing 4, 6
Cisco Unified Communications Manager 4
security, hypertext transfer protocol 6
buttons in GUI 18, 19, 20
Cisco Unified Communications Manager Administration 18, 19, 20

C

call display restrictions 252, 541, 663
configuring in device profile 663
configuring in translation pattern 663
phone configuration 541
Call park 327
  described 327
call pickup group 328
  described 328
call routing 263
  directory numbers 263
  configuration overview 263
call waiting 265
  configuration settings 265
Called Party Tracing 416
called party transformation patterns 315
  configuration settings (table) 315
  related topics 315
calling party transformation patterns 311
  configuration settings (table) 311
  related topics 311
calling search spaces 247, 248, 291
  configuration overview 247
  configuration settings (table) 247
  configure display in drop-down list box 291
  partition limitations 248
  related topics 247
Cisco CallManager service 37, 38
  activating 37
  deactivating 38
Cisco Unified Communications Manager 3, 4, 5, 6, 21, 22, 25, 33, 37, 39, 42, 743
  accessibility 21, 22
  benefits 4
  browsing into 4
  configuration settings (table) 33
  configuring 33
  groups 39, 42
    configuration overview 39
    configuration settings (table) 39
    synchronizing configuration 42
  introduction 3, 743
  key features 4
  login 5
  logout 6
  more information 22
  overview 3, 743
  related topics 3, 33
  server configuration 25
  synchronizing configuration 37
Cisco Unified Communications Manager Administration 7, 8, 10, 11, 12, 14, 15, 16, 17, 18, 19, 20, 21
  adding records 17
  buttons in GUI 18, 19, 20
  Cisco Unified Presence Server link 20, 21
  copying records 17
  customized login message 21
  deleting records 16
  finding records 16
  (continued)
Cisco Unified Communications Manager Administration (continued)
  FireFox 3.x and HTTPS 10
  GUI 14, 15
  icons in GUI 18, 19, 20
  Internet Explorer 7 and HTTPS 7
  Internet Explorer 8 and HTTPS 8
  last successful login message 21
  navigating 14
  Safari 4.x and HTTPS 11
  using Help 16
Cisco Unified IP Phone Services 583, 584
  configuring 583
  subscribing 583
  unsubscribing 584
  updating 584
Cisco Unified IP Phones 537, 577, 581, 588, 589, 590, 879
  configuration overview 537
  configuring 577
  displaying MAC address 590
  finding actively logged in devices 588
  finding remotely logged-in devices 589
  related topics 537
  synchronizing configuration 581
  that are running SIP 879
  third-party device differences 879
Cisco Unified Presence Server 20, 21
  link from Cisco Unified Communications Manager Administration 20, 21
Cisco Unity 765
  adding an administrator to 765
Cisco Unity Connection 295, 765, 779
  adding an administrator to 765
  user configuration voice mailbox 779
  voice mailbox 295
  directory numbers 295
Cisco voice mail 387
  configuration overview 387
Cisco voice mail port wizard 395
Cisco voice-mail pilot 407
  configuration overview 407
  related topics 407
client matter codes 327
  described 327
CMLocal date/time group 47
  common device configuration 719
  synchronizing configuration to applicable devices 719
  common device configurations 713, 714
    configuration overview 713
    configuration settings (table) 714
  common phone profile 725
  synchronizing configuration to applicable devices 725
  common phone profiles 721
  configuration settings (table) 721
common phone profiles (continued)
  configuring 721
  related topics 721
conference bridges 337, 339, 341, 343, 345, 348, 350, 352, 354, 355
  Cisco Conference Bridge (WS-SVC-CMM) 348
  configuration settings (table) 348
Cisco IOS 343
  configuration settings (table) 343
Cisco IOS Guaranteed Audio Video Conference Bridge 352
  configuration settings (table) 352
Cisco IOS Heterogeneous Video Conference Bridge 350
  configuration settings (table) 350
Cisco IOS Homogeneous Video Conference Bridge 354
  configuration settings (table) 354
Cisco TelePresence MCU 355
  configuration settings (table) 355
Cisco video 345
  configuration settings (table) 345
configuration overview 337
hardware 341
  configuration settings (table) 341
related topics 337
software 339
  configuration settings (table) 339
conference devices 361
  synchronizing configuration 361
configuring 293
copying records 17
  Cisco Unified Communications Manager Administration 17
credential policy 755
  configuration overview 755
  configuration settings (table) 755
related topics 755
credential policy default 751, 753
  assigning 753
  configuration overview 751
  configuration settings (table) 751
configuring 753
related topics 751
CTI route points 421, 422, 426
  configuration overview 421
  configuration settings (table) 422
related topics 421
  synchronizing configuration 426
custom phone button templates 673
  creating an expansion module 673

cdate/time group 50
  synchronizing configuration to applicable devices 50
date/time groups 43, 47
  configuration overview 47
  configuration settings (table) 47
related topics 47
  using phone NTP reference configuration with 43
default device profiles 657
  configuration overview 657
  configuration settings (table) 657
related topics 657
defaults 651, 652, 655
  configuration overview 651
  configuration settings (table) 651, 652
  devices 651, 652, 655
related topics 651
  updating 652
  with non-firmware loads 655
deleting records 16
  Cisco Unified Communications Manager Administration 16
dependency records 873, 874, 876
  accessing 874
  buttons 876
detail example (figure) 874
disabling 874
enabling 873
terprise parameter 873
overview 873
  summary example (figure) 874
device defaults 651, 652
  configuration overview 651
  configuration settings (table) 651, 652
related topics 651
  updating 652
device mobility groups 146
  configuration overview 146
device mobility info 146
  configuration overview 146
device pools 63, 79
  configuration overview 63
  configuration settings (table) 63
related topics 63
  synchronizing configuration to applicable devices 79
device profiles 663
  configuration overview 663
  configuration settings (table) 663
related topics 663
devices 63, 403, 429, 433, 537, 577, 591, 655
  Cisco Unified IP Phones 537, 577
  configuration overview 537
  configuring 577
related topics 537
defining common characteristics 63
firmware load information 655
  configuration overview 655
related topics 655
FXO ports 526
FXS ports 525

g. clear codec 495
   enable 495

gatekeepers 429, 432
   configuration overview 429
   configuration settings (table) 429
   related topics 429
   synchronizing configuration 432
gateways 433, 435, 458, 463, 464, 467, 475, 495, 502, 515, 517, 518, 519, 522, 523, 525, 526, 527, 528, 529, 530, 531, 532, 534
   adding 522
   analog access configuration settings (table) 458
   analog access gateway, adding 532
   BRI configuration settings (table) 502
   Cisco IOS SCCP gateway configuration settings (table) 464
   Cisco VG224/VG248 analog gateway, adding 532
   Cisco VG224/VG248 analog ports, adding 532
   Cisco VG248 configuration settings (table) 463
   configuration overview 433
   configuration settings (table) 433
   Digital Access PRI configuration settings (table) 475
   E & M port configuration settings (table) 519
   enabling g.clear codec 495
   FSX/FXO configuration settings (table) 467
   ground start port configuration settings (table) 518
   H.323 configuration settings (table) 438
   H.323, adding 531
   ISDN 475
   ISDN BRI 502
   loop start port configuration settings (table) 517
   MGCP 435, 502, 523, 525, 526, 527, 528
      BRI ports, adding 528
      BRI, configuring 502
      Cisco IOS, adding 523
      configuration settings (table) 435
      Digital Access PRI ports, adding 528
      FXO ports, adding 526
      FXS ports, adding 525
      ports, adding 525
      T1 ports, adding 527
      modifying 534
      non-IOS, adding 530
      port configuration settings (table) 467
      ports, adding 532
      POTS port configuration settings (table) 515
      PRI 475
      related topics 433

gateways (continued)
SCCP 529
   Cisco IOS, adding 529
   synchronizing configuration 534
   updating 534

groups 39, 47, 145
   BLF presence, configuring 145
   Cisco Unified Communications Manager 39
      configuration overview 39
      configuration settings (table) 39
   date/time 47
      configuration overview 47
      configuration settings (table) 47
      related topics 47

GUI 14, 15
   Cisco Unified Communications Manager Administration 14, 15

H
H.323 531
   adding gateways 531
Help 16
   Cisco Unified Communications Manager Administration 16
      using 16
HTTPS 6
   HTTP over secure sockets layer 6
hunt list 209, 210, 211, 212, 213, 214
   adding 210
   adding line groups 211
   changing the order of line groups 213
   configuration overview 209
   deleting 214
   finding 210
   related topics 209
   removing line groups 212
   synchronizing configuration to affected devices 213
hunt pilots 215
   configuration overview 215
   configuration settings (table) 215
   related topics 215

I
icons in GUI 18, 19, 20
   Cisco Unified Communications Manager Administration 18, 19, 20
intercom 325, 326
   calling search spaces 326
      configuration overview 326
intercom (continued)
directory numbers 326
  configuration overview 326
partitions 325
  configuration overview 325
translation patterns 326
  configuration overview 326
introduction to Cisco Unified Communications Manager 3, 743
IP address 25
IP Phone Services, See Cisco Unified IP Phone Services
ISDN 475
  gateway configuration 475
ISDN BRI 502
  gateway configuration 502
IVR 384

L

LDAP 89, 93, 101, 105
  authentication 101
    configuration settings (table) 101
    configuring 101
    related topics 101
directory 93
  configuration settings (table) 93
  configuring 93
  related topics 93
filter 105
  configuration settings (table) 105
  configuring 105
  related topics 105
system 89
  configuration settings (table) 89
  configuring 89
  related topics 89
licensing 881
  third-party phones that are running SIP 881
line groups 201, 207
  adding members 207
  configuration overview 201
  configuration settings (table) 201
  related topics 201
  removing members 207
locations 107
  configuration overview 107
  configuration settings (table) 107
  related topics 107
login 5
  Cisco Unified Communications Manager 5
login message 21
  customized 21
  last successful login 21
logout 6
  Cisco Unified Communications Manager 6

M

max list box enterprise parameter 291
calling search space 291
media resource group lists 375
  configuration overview 375
  configuration settings (table) 375
  related topics 375
media resource groups 371
  configuration overview 371
  configuration settings (table) 371
  related topics 371
media termination point 363
  See MTP 363
meet-me number patterns 297
  configuration overview 297
  configuration settings (table) 297
  related topics 297
message waiting 403
  configuration overview 403
  configuration settings (table) 403
  related topics 403
MGCP 502, 523, 525, 526, 527, 528, 530
  BRI gateway configuration settings (table) 502
Cisco IOS, adding 523
  Digital Access PRI ports, adding 528
  Digital Access T1 ports 527
  FXO ports, adding 526
  FXS ports, adding 525
gateways, adding 523
  non-IOS gateway, adding 530
  ports, adding 525
migrating phone settings 579
MLPP domains 119, 121
  configuration settings (table) 119
  overview 119
  related topics 119
  resource priority namespace network domain 121
mobile connect 326, 329, 384, 739
  access list 326
  mobile voice access 384
  mobility configuration 329
  remote destination 739
  remote destination profile 739
mobile voice access 384, 739
  configuration 384
  IVR 384
  remote destination 739
  remote destination profile 739
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
</table>

mobility configuration 329
MTP 363, 364, 365
  configuration overview 363
  IOS configuration settings (table) 364
  related topics 363
  synchronizing configuration 365
MWI 403
  configuration settings (table) 403
  related topics 403

N
navigating 14
  Cisco Unified Communications Manager Administration 14
Network Time Protocol, See phone NTP reference
normalization 733, 737
  configuration settings (table) 733
  importing scripts 737
  related topics 733
number patterns 297
  configuration settings (table) 297
  meet-me 297
  related topics 297

O
overview of Cisco Unified Communications Manager 3, 743

P
parameters 127, 131, 133
  configuring 131
  configuring for a service 131, 133
  displaying for a service 133
  enterprise 127
  related topics 131
partitions 241, 242, 244, 377
  calling search space limitations (table) 242
  configuration overview 241
  configuration settings (table) 241
  related topics 241, 377
  searching 244
  synchronizing configuration to applicable devices 244
phone button templates 587, 671, 673
  configuration overview 671
  configuration settings (table) 671
  creating an expansion module 671
  modifying button items 587
  related topics 671
phone NTP reference 43
  configuration settings (table) 43
  overview 43
  related topics 43
phone services 683, 688, 691, 692, 693
  adding to a phone button 693
  Cisco-provided default services 689
  configuration overview 683
  configuration settings (table) 683
  configuring Cisco-signed Java MIDlets 683
  related topics 683
  service parameters 688, 691, 692
    configuring 691
    deleting 692
    settings (table) 688
phones 539, 579, 581, 588, 589, 590, 799, 802
  adding with end user 802
  configuration settings (table) 539
  configuring with end user 799
  displaying MAC address 590
  finding actively logged in devices 588
  finding remotely logged-in devices 589
  migrating phone settings to different phone 579
  phone migration settings (table) 579
  synchronizing configuration 581
physical locations 146
  configuration overview 146
PLAR 293
plug-ins 745, 746
  configuration overview 745
  installing 746
  related topics 745
  updating the URL 746
  URL configuration settings (table) 745
ports 495, 534
  Digital Access T1 configuration settings (table) 495
  modifying 534
  updating 534
PRI 475
  gateway configuration 475

R
recording profiles 731
  overview 731
  related topics 731
regions 53, 55, 61
  configuration settings (table) 55
  configuring 53
  related topics 53
  synchronizing configuration to applicable devices 61
### Related Topics
- **Cisco Unified Communications Manager**: 3
- **Remote Destination**: 739
- **Remote Destination Profile**: 739
- **Resource Priority**: 121, 123
  - Namespace List: 123
    - Configuration Settings: 123
      - Overview: 123
    - Related Topics: 123
  - Namespace Network Domain: 121
    - Configuration Settings: 121
      - Overview: 121
    - Related Topics: 121
- **Roles**: 787, 796, 797
  - Assigning to User Groups: 796
    - Configuration Settings (Table): 787
    - Described: 787
    - Related Topics: 787
  - Viewing for a User: 797
- **Route Filters**: 169, 171, 172, 173
  - Adding Clauses: 171
    - Configuration Overview: 169
    - Configuration Settings (Table): 169
    - Editing Clauses: 171
    - Operators: 173
      - Described (Table): 173
      - Explained: 173
    - Related Topics: 169
  - Removing Clauses: 172
  - Synchronizing Configuration to Applicable Devices: 172
  - Tags: 173
    - Described (Table): 173
    - Explained: 173
- **Route Groups**: 177, 180, 181
  - Adding Devices: 180
    - Configuration Overview: 177
    - Configuration Settings (Table): 177
    - Related Topics: 177
  - Removing Devices: 181
- **Route Lists**: 183, 185, 187, 188
  - Adding Route Groups: 185
    - Changing the Order of Route Groups: 187
    - Configuration Overview: 183
    - Related Topics: 183
  - Removing Route Groups: 187
  - Synchronizing Configuration to Affected Devices: 188
- **Route Patterns**: 189, 227
  - Configuration Overview: 189
  - Configuration Settings (Table): 189
  - Related Topics: 189
  - SIP: 227
    - See SIP Route Patterns: 227
      - Configuration Overview: 305
  - Configuration Overview: 305

### S
- **SCCP**: 529
  - Cisco IOS, Adding: 529
  - Gateways, Adding: 529
  - Scripts: 733, 737
    - Configuration Settings (Table): 733
    - Importing: 737
    - Related Topics: 733
- **Security Profile**: 147
  - Configuring for CUMA: 147
  - Configuring for Phone: 147
  - Configuring for SIP Trunk: 147
- **Servers**: 25
  - Configuration Settings (Table): 25
  - Configuring: 25
  - Related Topics: 25
  - **Service Parameters**: 131, 133
    - Configuring: 131
    - Configuring for a Service: 131, 133
    - Displaying for a Service: 133
    - Related Topics: 131
  - **Service URL Button**: 585
    - Adding: 585
  - **Services**: 37, 38, 683, 688, 691, 692, 693
    - Cisco CallManager: 37, 38
      - Activating: 37
      - Deactivating: 38
    - Phone: 683, 688, 691, 692, 693
      - Adding to a Phone Button: 693
      - Configuration Overview: 683
      - Configuration Settings (Table): 683
      - Deleting a Service Parameter: 692
      - Related Topics: 683
      - Service Parameter: 691
      - Service Parameter Settings (Table): 688
  - **SIP**: 877, 879, 880
    - Configuration Differences: 879
    - Configuring Third-Party Phones: 877
    - Third-Party Phones that are Running SIP: 877
      - Configuration Checklist (Table): 877
    - Third-Party Phones that are Running SIP and TFTP: 880
    - SIP Dial Rules: 161, 165, 166, 167, 168
      - Configuration Settings (Table): 161
      - Configuring: 161
SIP dial rules (continued)
  dial plan examples 166
  pattern formats 165
  related topics 161
  resetting 167
  synchronizing configuration with affected SIP phones 168
SIP normalization scripts 733, 737
  configuration settings (table) 733
  importing 737
  related topics 733
SIP profiles 695, 696, 711
  configuration settings 695
  configuring 695
  related topics 695
  resource priority namespace list 696
  synchronizing configuration 711
SIP route patterns 227
  configuration settings (table) 227
  configuring 227
  related topics 227
softkey template configuration 681
  synchronizing configuration to applicable devices 681
softkey templates 675, 676, 677, 678, 679, 680, 681, 682
  adding application softkeys 677
  assigning to phones 682
  configuration overview 675
  creating 676
  deleting 680
  finding 675
  modifying 679
  related topics 675
  renaming 679
  softkey positions 678
  updating 681
speed dial configuration settings (table) 570
speed-dial buttons 582
  configuring 582
SRST 115
  configuration overview 115
  configuration settings (table) 115
  related topics 115
Survivable Remote Site Telephony, See SRST

T
T1 ports 527
  adding 527
templates 671, 675, 676, 677, 678, 679, 680, 681, 682
  phone button 671
    configuration overview 671
    configuration settings (table) 671
    related topics 671
templates (continued)
  softkey 675, 676, 677, 678, 679, 680, 681, 682
    adding application softkeys 677
    assigning to phones 682
    configuration overview 675
    creating 676
    deleting 680
    finding 675
    modifying 679
    related topics 675
    renaming 679
    softkey positions 678
    updating 681
TFTP 880
  third-party phones that are running SIP 880
third-party phones 881
  SIP 881
    licenses 881
time periods 233
  configuration overview 233
  configuration settings (table) 233
  related topics 233
time schedules 237
  configuration overview 237
  configuration settings (table) 237
  related topics 237
time zones 47
transcoders 367, 369
  configuration overview 367
  configuration settings (table) 367
  related topics 367
  synchronizing configuration 369
translation patterns 251, 252
  called party configuration settings (table) 251
  calling party configuration settings (table) 251
  related topics for called party 251
  related topics for calling party 251
trunks 591, 645, 646, 647, 648, 649
  configuration overview 591
  configuration settings (table) 591
  configuring 646
  deleting 647
  finding 645
  related topics 591
  resetting 648
  synchronizing configuration 649
user/phone add (continued)
related topics 799

voice mail 387, 395, 396, 397, 399, 400, 401, 403, 411, 413
adding a new server and ports 396
adding ports with the wizard 400
configuration overview 387
deleting ports with the wizard 401
message waiting overview 403
port configuration settings (table) 387
port wizard configuration overview 395
port wizard directory number configuration settings 399
port wizard related topics 395
profile configuration overview 411
related topics 387
synchronizing profile configuration to applicable devices 413
voice-mail profiles configuration settings (table) 411

voice-mail pilot 407
configuration overview 407
configuration settings (table) 407
related topics 407

voice-mail profiles 411
configuration overview 411
configuration settings (table) 411
related topics 411

web browsers 4