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 and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers 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](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)

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xvii

Purpose xvii
Audience xvii
Conventions xvii
Related Documentation xviii
Obtaining Documentation and Submitting a Service Request xix

CHAPTER 1 Configuration 1

Fulfillment Procedures Overview 1
Example Fulfillment Procedures 1
Roles 2
Unicode Limitations 2

CHAPTER 2 Hierarchy Management 3

Cisco Unified Communications Domain Manager 10.6(1) Overview 3
View the Hierarchy 4
Create a Provider 5
Create Reseller 6
Create Customer 7
Create Intermediate Node 9
Delete a Hierarchy Node 10
Manage Local Administrators and Operators 11
Set Localization Language at Hierarchy Node 12

CHAPTER 3 Device Management 13

Create the HCM-F Device 13
Cisco Unified Communications Manager Configuration in Cisco Unified CDM 15
Set up Cisco Unified Communications Manager Servers 16
Set up IM and Presence Service Servers 18
CUP Cluster Migration 19
  Migrate CUP to a Cisco Unified Communications Manager Cluster 20
Cisco Unified Communications Manager Server Deletion 21
Configure Regions 21
Delete Region 22
Set up Cisco Unity Connection 23
  Cisco Unity Connection Server Deletion 25
Set up Cisco Emergency Responder 25
  Associate CER with Customers 26
  View Associated Clusters on CER Servers 27
Set up Cisco WebEx 27
Set up Customer Equipment 28
Prime Collaboration Assurance Integration with Cisco Unified Communications Domain Manager 10.6(1) 29
Enable a Scheduled Data Sync 30
Manually Run the Default Data Sync 31
Controlling a Data Sync with a Model Type List 31
  Create a Targeted Model Type List 33
  View List of Device Models 33
  Create a Custom Data Sync 34

CHAPTER 4
Customer Configuration 35
  Configure Network Device List 35
  Network Device List Selection Rules 36

CHAPTER 5
Site Management 39
  Create Site 39
  Modify Site Defaults 40
  Cisco Hosted Collaboration Solution Roles and Privileges 44

CHAPTER 6
Set Up Northbound Notification 47
  Northbound Notification 47
  Notification Format 48
CHAPTER 7 LDAP Management 53
- Enable LDAP Integration 53
- Set Up LDAP User Sync 54
- Sync Users from LDAP 55

CHAPTER 8 User Management 57
- User Management Overview 58
- Create User 58
- Manage Local Administrators and Operators 59
- Define a Filter 60
- Methods to Push Users to Cisco Unified Communications Manager 61
- Automatic User Push to Cisco Unified Communications Manager 61
- Manual User Push to Cisco Unified Communications Manager 62
- Automatic Cisco Unified Communications Manager User Move 63
- Move Users 64
- Check User Provisioning Status 65
- Sync and Purge LDAP Users 65
- Sync Cisco Unified Communications Manager Users, Lines, and Phones 66
- Manage Duplicate User Names 67
- Assign a Credential Policy to a User 68
- Assign a Credential Policy to an Administrator 69
- Unlock a Locked Out User 69
- Unlock a Locked Out Administrator 69
- Manually Disable User Account 70
- Manually Disable Administrator Account 70
- Password Management 71
  - User Synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1) 71
  - User Synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1) (SSO Enabled) 71
User Synced from LDAP to Cisco Unified Communications Manager 71
User Synced from Cisco Unified Communications Domain Manager 10.6(1) 72
User Added Manually from User Management 72
Force User Password Change 72
Force Administrator Password Change 73
Manage Your Own Account Password 73
Change Your Own Password 74
Reset Your Own Password 74
Configure Your Own Password Reset Questions 75
Self Service 75
Self Service and End User Configuration 76

CHAPTER 9  Single Sign On 79
SSO Certificate Management 79
Configure Single Sign-On for Cisco Unified Communications Domain Manager 80

CHAPTER 10  Entitlement Management 83
Entitlement Enforcement 83
Entitlement Workflow 85
Add Device Type 85
Create Device Group 85
Create an Entitlement Catalog 86
Create an Entitlement Profile 87

CHAPTER 11  Dial Plan Management 89
Dial Plan Example Workflow 90
Create a Customer Dial Plan 90
Create a Site Dial Plan 91
Configure Class of Service 93
Macros 94
Clone a Class of Service 96
Configure Short Code 96
Number Management 97
E164 Inventory Management 97
Add E164 Inventory 98
CHAPTER 12

Subscriber Management 173

Add Subscribers 173
Contents

CHAPTER 13 Services 203

Voice Mail 203

Create Voice Mail Service 203

Associate Voice Mail Services to Customer 205

Add Alternate Extension 206
Add Additional Notification Devices 206
Disassociate Voice Mail Services from Customers 207
Delete Voice Mail Service 207
Define a Voice Mail Pilot Number 207
Associate Pilot Numbers to a Site 208
Disassociate Pilot Numbers from a Site 209
Delete a Voice Mail Pilot Number 209
Setup Contact Center Using Cisco Unified Communications Manager 209
Set Up Contact Center Server 210
Set Up Contact Center Service 211
Configure Unified Mobile Agent 212
  Configure CTI Port 212
  Tag CTI Port as Contact Center Agent Line 213
Configure Cisco Media Sense 213
  Setup Trunk 213
  Setup Route Group 214
  Setup Route List 214
  Setup Route Patterns 215
  Configure Device 215
Set up Cisco Remote Silent Monitoring 216
  Create Unified CM Group 216
  Create Region 216
  Create Device Pool 217
  Create Phones 217

CHAPTER 14  Self Provisioning 219
Self-Provisioning Overview 219
Bottom-Up User Management 220
Top-Down User Management 220
Cisco Unified Communications Manager Configuration for Self-Provisioning 221
Site Configuration for Self-Provisioning 221
Generate User's Primary Line 221
Specify the Primary Line per Subscriber 222
Add Self-Provisioning Universal Device Template 222
Add Self-Provisioning Universal Line Template 224
Add Self-Provisioning User Profile 225
Set Default User Profile for Site 225
Add Self-Provisioning Line Mask 226

CHAPTER 15
Customizations 227
Common Tasks 227
Clone 228
Create a Clone 228
Selecting Items 228
Ordering Lists 229
Filtering Lists 229
Navigating Lists 229
Updating on Pop-up Screens 230
Role Management 230
Clone a Role 231
Create a Service Assurance Only Role 231
Create a Fulfillment Only Role 232
Deploy a Customized Credential Policy 232
Session Timeout Rules 235
GUI Customization 235
Themes 235
Download, Edit and Update a Theme 236
Add a Theme 237
Theme Field Reference 237
Theme Settings Reference 238
Set the Login Page Theme 239
Menu Layouts 239
Create a Menu Layout 240
Menu Layout Field Reference 240
Landing Pages 241
Create a Landing Page 241
Landing Page Field Reference 242
Landing Page Definition 244
Field Display Policies 246
Clone a Field Display Policy 247
Field Display Policy Field Reference 247
Configuration Templates 248
Clone a Configuration Template 249
   Configuration Template Field Reference 249
Access Profiles 250
Clone an Access Profile 250
   Access Profile Field Reference 250

CHAPTER 16  Bulk Loading 253
   Bulk Loading a File 253

CHAPTER 17  Backup and Restore 255
   Backups 255
      Backup Destinations 255
      Create Space for a Backup or Restore 256
      Adding More Space to Accommodate a Large Restore 256
      Backup Passphrase 256
      Setting up the Backup Passphrase on a New Environment 257
      Reassign Current Drives (Backup and DBroot) 257
      Create a Backup 257
      Restore the Backup 258
      Restore a Backup in a Clustered Environment 259
      Example of a Successful Restore 259
      Maintaining Backups 260
      Exporting Backups 260
      Scheduling 260
      DR Failover 261
      DR Failover and Recovery 261
         DR Failover and Recovery Scenarios 261
            Scenario: Loss of a Non-primary Node in the Primary Site 262
            Scenario: Loss of a Non-primary Server in the DR Site 263
            Scenario: Loss of the Primary Database Server 265
            Scenario: Loss of a Primary Site 266
            Scenario: Loss of a DR Site 268
      High Availability Disaster Recovery 270
<table>
<thead>
<tr>
<th>Chapter 18</th>
<th>System Maintenance</th>
<th>275</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Maintenance</td>
<td>275</td>
<td></td>
</tr>
<tr>
<td>Cluster Failure Scenarios</td>
<td>276</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 19</th>
<th>Networking</th>
<th>279</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Interfaces</td>
<td>279</td>
<td></td>
</tr>
<tr>
<td>Network services</td>
<td>279</td>
<td></td>
</tr>
<tr>
<td>Network URI specification</td>
<td>280</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 20</th>
<th>Monitoring</th>
<th>281</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Control</td>
<td>281</td>
<td></td>
</tr>
<tr>
<td>Application control</td>
<td>281</td>
<td></td>
</tr>
<tr>
<td>Application Status</td>
<td>281</td>
<td></td>
</tr>
<tr>
<td>Starting and Stopping</td>
<td>282</td>
<td></td>
</tr>
<tr>
<td>Remote Execution in Clusters</td>
<td>282</td>
<td></td>
</tr>
<tr>
<td>Notifications</td>
<td>283</td>
<td></td>
</tr>
<tr>
<td>Warnings and Notifications</td>
<td>283</td>
<td></td>
</tr>
<tr>
<td>SNMP queries</td>
<td>283</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 21</th>
<th>System Control</th>
<th>285</th>
</tr>
</thead>
<tbody>
<tr>
<td>System restart</td>
<td>285</td>
<td></td>
</tr>
<tr>
<td>Passwords</td>
<td>285</td>
<td></td>
</tr>
<tr>
<td>File Management</td>
<td>286</td>
<td></td>
</tr>
<tr>
<td>Drive control</td>
<td>286</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 22</th>
<th>System Security</th>
<th>289</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>289</td>
<td></td>
</tr>
</tbody>
</table>
Security Patches and Updates 290
Using Your Own Repository Mirrors 290
Configuration Encrypted 291
Backup Encrypted 291
Application Install Files Encrypted 291
Protected Application Environments (Jails) 292
Restricted User Shell 292
Creating Additional Users 292
Granting and revoking user rights 293
Password Strength Rules 294
SSH key management 294

CHAPTER 23

Network Security 295
Network Communications between Nodes within the Cluster 295
Network Communications External to the Cluster 297
Dynamic Firewall 298
Service and Ports list 298
Web Certificates 299
Web Certificate Expiration Notice 299
Set Up a Web Certificate 300
Web Certificate Commands 300
Network URI specification 300

CHAPTER 24

Macros 303
Macros 304
Macro Syntax Brackets 304
Dot notation 305
SELECT FROM WHERE Macro Syntax 306
Macro Nesting 310
Macro Syntax to Filter by Meta Properties 310
Numeric Functions 312
String Functions 312
List Functions 314
Rule Filter Functions 317
Macro Function 319
CHAPTER 25

SNMP 339

Introduction to SNMP and MIB 339
SNMP Traps 341
Management Information Bases 343
MIB and Trap Details 344

SNMPv2-MIB - RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) 344
IF-MIB - RFC 2863 - The Interfaces Group MIB 344
MIB-II - RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets 345
IP-MIB - RFC 4293 - Management Information Base for the Internet Protocol (IP) 345
TCP-MIB - RFC 4022 - Management Information Base for the Transmission Control Protocol (TCP) 345
UDP-MIB - RFC 4113 - Management Information Base for the User Datagram Protocol (UDP) 346
HOST-RESOURCES-MIB - RFC 2790 - Management Information Base for Host Resources 346
SNMP Traps: System Startup 347
SNMP Traps: Service Startup Changes Made 348
SNMP Traps: Service Monitoring - Changes Made 348
SNMP Traps: System Shutdown 349
SNMP Trap: Disk Full 349
SNMP Trap: Excessive Load 350
SNMP Trap: Backup 352
SNMP Trap: Health Emails 353
SNMP Trap: Disk Latency 353
SNMP Trap: Mailbox Status 354
SNMP Trap: Cluster Status 355
SNMP Trap: Database Failover Status 356
SNMP Trap: Large Log Files 356
SNMP Trap: Network Status 357
SNMP Trap: Security Updates 358
SNMP Trap: Memory Usage 358
SNMP Trap: NTP Status 359
SNMP Trap: DNS status 360
SNMP Trap: Domain Status 361
SNMP Trap: NTP Offset 361
SNMP Trap: Process Memory Threshold Status 362

APPENDIX A

MIB List 363

MIB List 363
Preface

• Purpose, page xvii
• Audience, page xvii
• Conventions, page xvii
• Related Documentation, page xviii
• Obtaining Documentation and Submitting a Service Request, page xix

Purpose

The purpose of this document is to provide the user with information to configure, maintain and operate their Cisco Unified Communications Domain Manager 10.6(1) server.

Audience

This document provides information for service providers who manage. This guide requires knowledge of the Cisco Hosted Collaboration Solution (HCS).

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</td>
</tr>
<tr>
<td>bold font</td>
<td>Commands and keywords and user-entered text appear in bold font.</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><em>Italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td><strong>Courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td><strong>Bold Courier</strong> font</td>
<td><strong>Bold Courier</strong> font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive non-bolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>string</td>
<td>A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Non-printing characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Related Documentation**

The following documents have been issued for Cisco Unified Communications Domain Manager 10.6(1):

- Cisco Unified Communications Domain Manager, Release 10.6(1) Planning and Install Guide
- Cisco Unified Communications Domain Manager, Release 10.6(1) Maintain and Operate Guide
- Cisco Unified Communications Domain Manager, Release 10.6(1) API Reference Guide
- Cisco Unified Communications Domain Manager, Release 10.6(1) Bulk Loader Provisioning Guide
The following resources may also be useful:

- **Cisco Hosted Collaboration Solution, Release 10.6(1) Install Guide**
- **Installing and Configuring Cisco HCS for Contact Center**: https://communities.cisco.com/docs/DOC-38566
- Cisco HCS developer guides: http://developer.cisco.com/web/hcs
- AXL Developer documentation: http://developer.cisco.com/web/axl/
- **Cisco Unified Communications Manager IM and Presence Developer Guide**: https://developer.cisco.com/site/devnet/home/index.gsp
- **Cisco Contact Center Domain Manager Web Services Reference**: https://communities.cisco.com/docs/DOC-33790.

### Obtaining Documentation and Submitting a Service Request


Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.
CHAPTER 1

Configuration

- Fulfillment Procedures Overview, page 1
- Example Fulfillment Procedures, page 1
- Roles, page 2
- Unicode Limitations, page 2

Fulfillment Procedures Overview

The primary objective of using Cisco Unified Communications Domain Manager 10.6(1) is to easily onboard Customers and End Users with Collaboration Services. The fulfillment procedures to achieve this objective may involve administrators at the provider, reseller, customer and site levels of the hierarchy. For more information about the hierarchy, see the Cisco Unified Communications Domain Manager, Release 10.6(1) Planning and Install Guide.

The following section shows a sample procedure for configuring Cisco Unified Communications Domain Manager 10.6(1).

Example Fulfillment Procedures

This is an example set of steps for onboarding customers and end users. Customization and some optional configuration are not included in this example.

Note

Shared applications are configured at the Provider or Reseller level. Dedicated applications at the Customer level.

Before You Begin

HCM-F and any UC Applications to be used for provisioning customer sites and users must be installed and ready.

For WebEx Cloud, the necessary licenses and accounts must be available for provisioning.
**Roles**

The system has a powerful Role Based Access framework which ties a User Role to Menu Layouts, Access Profiles, Landing Pages and Themes. The system comes with a default set of Roles, Menu Layouts, Access Profiles, Landing Pages and Themes. The default set of roles in the system are HCS Admin, Provider, Reseller, Customer, Site and End User.

For information about adding or modifying roles, see Role Management, on page 230.

**Unicode Limitations**

For Cisco Unified Communications Domain Manager 10.6(1), Unicode characters are supported only in the following fields:

- User Information in Cisco Unified Communications Domain Manager 10.6(1) User Management
- Description
- Contact Information (Address, City, State, Postal Code, Country, Extended Name, External Customer ID, Account ID and Deal IDs)
- Phone Label
Hierarchy Management

- Cisco Unified Communications Domain Manager 10.6(1) Overview, page 3
- View the Hierarchy, page 4
- Create a Provider, page 5
- Create Reseller, page 6
- Create Customer, page 7
- Create Intermediate Node, page 9
- Delete a Hierarchy Node, page 10
- Manage Local Administrators and Operators, page 11
- Set Localization Language at Hierarchy Node, page 12

Cisco Unified Communications Domain Manager 10.6(1) Overview

The major change in the configuration of Cisco Unified Communications Domain Manager from 8.x to 10.x is the location of the master data for different aspects of the solution. In 8.x deployments the master copy of all data was stored in the Shared Data Repository (SDR). Consequently any changes to the data had to be made in Cisco Unified Communications Domain Manager and then synchronized down to the UC Applications such as Cisco Unified Communications Manager. In 10.X the source of master data is distributed between domain manager and the call manager and a bi-directional sync can export and import data from the domain manager and the applications. This approach enables configuration changes to be made on either the domain manager or on the UC applications giving greater flexibility and enabling a faster resolution when problems occur.

The following chapters include content on provisioning Cisco Unified Communications Domain Manager 10.6(1) specifically as it relates to Customer Onboarding. This will include information on the provisioning steps and interactions between the domain manager and the various UC applications supported by Cisco HCS.

For more information on Cisco Unified Communications Domain Manager 10.6(1) see:

- Cisco Unified Communications Domain Manager 10.6(1) Planning and Install Guide
View the Hierarchy

An administrator can view the portion of the hierarchy that the administrator has access to. The provider administrator can view the complete hierarchy, while a customer admin can view only the customer, any intermediate nodes beneath the customer, and customer sites.

Procedure

Step 1

To view the hierarchy, select Hierarchy > Hierarchy Management.

A table containing the hierarchy nodes visible to the admin is displayed containing the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Node name</td>
</tr>
<tr>
<td>Description</td>
<td>Node description</td>
</tr>
<tr>
<td>Hierarchy Node Type</td>
<td>Indicates Provider, Reseller, Customer, or Site. Is blank for an intermediate node.</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>Shows the node location in the hierarchy in dot notation.</td>
</tr>
</tbody>
</table>

Step 2

To view a subset of the visible hierarchy, you can adjust the hierarchy path.

Example:
For instance, a provider admin, may set the path to point to a particular customer, and then will see only the hierarchy nodes for that customer.

**Step 3**
The hierarchy nodes can be sorted by clicking on the field headers. The hierarchy nodes can be searched by clicking the search icon on the field headers.

---

# Create a Provider

**Procedure**

1. **Step 1** Log in to Cisco Unified Communications Domain Manager 10.6(1) as hcsadmin@sys.hcs.
2. **Step 2** Select **Provider Management > Providers**.
3. **Step 3** Click **Add**.
4. **Step 4** Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the provider. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Once you enter a provider name, it cannot be changed.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Any spaces in the provider name will be converted to underscores in the</td>
</tr>
<tr>
<td></td>
<td>provider local administrator name and e-mail, if <strong>Create Local Admin</strong> is</td>
</tr>
<tr>
<td></td>
<td>checked.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the provider.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain of the provider. For example, provider.com. Used when creating</td>
</tr>
<tr>
<td></td>
<td>the default local admin user so the admin can log in with an email ID such as</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:ProviderAdmin@provider.com">ProviderAdmin@provider.com</a>. This field is mandatory.</td>
</tr>
<tr>
<td>Create Local Admin</td>
<td>Controls whether a default local administrator is created.</td>
</tr>
<tr>
<td>Cloned Admin Role</td>
<td>The HCS default provider role used to create a new role prefixed with the</td>
</tr>
<tr>
<td></td>
<td>provider name. The created provider role, shown in <strong>Default Admin Role</strong></td>
</tr>
<tr>
<td></td>
<td>field, is assigned to the default local admin. This field appears only if</td>
</tr>
<tr>
<td></td>
<td><strong>Create Local Admin</strong> is checked.</td>
</tr>
<tr>
<td>Default Admin Role</td>
<td>The created provider role that is assigned to the default local admin. This</td>
</tr>
<tr>
<td></td>
<td>field is read only and appears only if <strong>Create Local Admin</strong> is checked.</td>
</tr>
<tr>
<td>Default Admin Password</td>
<td>The password to assign to the default local admin. This mandatory field</td>
</tr>
<tr>
<td></td>
<td>appears only if <strong>Create Local Admin</strong> is checked.</td>
</tr>
</tbody>
</table>
Create Reseller

Creating a reseller is optional.

Before You Begin

During Cisco Unified Communications Domain Manager 10.6(1) installation, the hcsadmin Administrator must configure the HCM-F device and create the Provider. See Cisco Unified Communications Domain Manager, Release 10.6(1) Planning and Install Guide for details.

Procedure

Step 1  Log in to the server as the Provider admin.
Log in with the Provider admin's email address, which is case-sensitive. The hcsadmin Administrator can find the Provider admin's email address by selecting User Management > Local Admins and then clicking the Provider.

Step 2  Select Reseller Management > Resellers from the menu.

Step 3  Click Add.

Step 4  Complete the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the reseller. This field is mandatory.</td>
</tr>
<tr>
<td>Note</td>
<td>Once you enter a name, it cannot be changed.</td>
</tr>
<tr>
<td>Note</td>
<td>Any spaces in the reseller name will be converted to underscores in the reseller local administrator name and e-mail, if Create Local Admin is checked.</td>
</tr>
</tbody>
</table>

Description Field

Repeat Default Admin Password

Confirm the default local admin password. This mandatory field appears only if Create Local Admin is checked.

Step 5  Click Save.

The provider hierarchy node in Cisco Unified Communications Domain Manager 10.6(1), the ServiceProvider name in SDR, and optionally a default provider admin are created. All existing Cisco HCS System Administration level dial plan schema and schema groups are auto-cloned to the new provider. For more information on auto-cloning, see Cisco Hosted Collaboration Solution, Release 10.6(1) Dial Plan Management Guide for Cisco Unified Communications Domain Manager, Release 10.6(1).
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Domain</td>
<td>Reseller domain. This field is used to create an e-mail address for the reseller default local administrator, for example <a href="mailto:Reseller1Admin@reseller1.com">Reseller1Admin@reseller1.com</a>. If omitted, the domain of the provider is used.</td>
</tr>
<tr>
<td>Create Local Admin</td>
<td>Controls whether a default local administrator is created for the reseller.</td>
</tr>
<tr>
<td>Cloned Admin Role</td>
<td>The Provider role used to create a new role prefixed with the reseller name. The created reseller role, shown in Default Admin Role field, is assigned to the default local admin user. This field appears only if Create Local Admin is checked.</td>
</tr>
<tr>
<td>Default Admin Role</td>
<td>The created reseller role that is assigned to the default local admin. This field is read only and appears only if Create Local Admin is checked.</td>
</tr>
<tr>
<td>Default Admin Password</td>
<td>The password to assign to the default local admin. This field appears and is mandatory only if Create Local Admin is checked.</td>
</tr>
<tr>
<td>Repeat Default Admin Password</td>
<td>Confirm the default local admin password. This field appears and is mandatory only if Create Local Admin is checked.</td>
</tr>
</tbody>
</table>

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

---

**Create Customer**

**Procedure**

**Step 1**  
Log in to server as the provider or reseller admin, depending on what organization will manage the customer. Log in with the provider or reseller admin's email address, which is case-sensitive. The provider admin can find the reseller admin's email address by selecting **User Management > Local Admins** and then clicking the reseller.

**Step 2**  
If logged in as a provider, and the customer is to be added under a reseller, set the hierarchy path to the reseller.

**Step 3**  
Select **Customer Management > Customers**.

**Step 4**  
Click **Add**.

**Step 5**  
Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Name</td>
<td>The name of the customer. This field is mandatory.</td>
</tr>
<tr>
<td>Note</td>
<td>Any spaces in the customer name will be converted to underscores in the customer local administrator name and e-mail, if Create Local Admin is checked.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Description | Customer description
Extended Name | The Extended Name can be used to provide a more descriptive name of the customer, and can be used by external clients to correlate their own customer records with the customer records stored in HCS. This Extended Name value is synced to the Customer record in the Shared Data Repository (SDR).
The Extended Name is not referenced by other components in HCS.
External Customer ID | The External Customer ID is used by the Service Inventory service. The External Customer ID is included as a column in the customer record of the service inventory report. Specify an External Customer ID in this field that matches the customer ID used by the external inventory tool which receives the Service Inventory reports. If the Service Inventory service is not being used, this field is not required. However, it can be used to correlate customer records in external systems with customer records in HCS.
Domain Name | Customer domain. This field is used to create e-mail addresses for:
- The customer default local administrator, for example: Customer1Admin@customer1.com
- Site default local administrators under the customer, for example: Site1Admin@customer1.com
If the customer domain is omitted, the provider domain (or reseller domain, if the customer is under a reseller in the hierarchy and the reseller domain was provided) is used instead.
Create Local Admin | Controls whether a default local administrator is created for the customer.
Cloned Admin Role | The Provider or Reseller role used to create a new role prefixed with the customer name. The created customer role, shown in Default Admin Role field, is assigned to the default local admin user. This field appears only if Create Local Admin is checked.
Default Admin Role | The created customer role that is assigned to the default local admin. This field is read only and appears only if Create Local Admin is checked.
Default Admin Password | The password to assign to the default local admin. This field appears and is mandatory only if Create Local Admin is checked.
Repeat Default Admin Password | Confirm the default local admin password. This field appears and is mandatory only if Create Local Admin is checked.
Account ID | The Account ID can be used by external clients to correlate their own customer records with the customer records stored in HCS. This Account ID value is synced to the Customer record in the Shared Data Repository.
The Account ID can be used by external clients to correlate their own customer records with the customer records stored in HCS. This Account ID value is synced to the Customer record in the Shared Data Repository.
Deal IDs are used by the Hosted License Manager (HLM) service which can be activated on the Hosted Collaboration Management Fulfillment (HCM-F) server. HLM supports Point of Sales (POS) report generation. The report includes all customers on the system with aggregate license consumption at customer level. The optional Deal ID field associated with the customer will be included in the report. Each customer can have zero or more Deal IDs. The Deal ID field is free text format and each deal ID should be separated by a comma.

Prime Collaboration is the application which monitors equipment used by this customer. Available Prime Collaboration applications must first be configured using the HCM-F User Interface, refer to Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1) for more information. Then HCM-F synchronization must be executed on Cisco Unified Communications Domain Manager 10.6(1). After the HCM-F data syncs into Cisco Unified Communications Domain Manager 10.6(1), available Prime Collaboration applications will appear in this dropdown. Select an available Prime Collaboration application to monitor Unified Communications applications and customer equipment configured for this customer.

Indicates whether the customer can use Shared UC Apps. If checked, the customer sites can use Network Device Lists that contain Shared UC Apps. Shared UC Apps are UC Apps that are defined above the Customer hierarchy level.

Step 6 Click Save.

Note When deleting a customer, you must remove any entities associated with the customer like LDAP, SSO providers, Devices and NDLs.

Create Intermediate Node

An intermediate node is an optional node in the Cisco Unified Communications Domain Manager 10.6(1) hierarchy that is located between the standard hierarchy nodes: provider, reseller, customer, and site. An intermediate node can be used to logically group other nodes. Intermediate nodes can be used to restrict access by administrators to a defined subset of nodes.

For example, intermediate nodes could be used to group customers by industry, or sites by geography.

When an intermediate node is created, no default administrator is created for it. Adding an administrator for an intermediate node is a separate step.

Procedure

Step 1 Login as an administrator at the level under which you want to create the intermediate node. For example, to create an intermediate node to group sites, log in as the customer administrator.
Delete a Hierarchy Node

Step 2  Select Hierarchy Management > Hierarchy.

Step 3  To add an intermediate node, click Add.

Step 4  Enter the following information for the node:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the node. This field is mandatory.</td>
</tr>
<tr>
<td></td>
<td>Note: Once you enter a name, it cannot be</td>
</tr>
<tr>
<td></td>
<td>changed.</td>
</tr>
<tr>
<td>Description</td>
<td>A detailed description of the node.</td>
</tr>
</tbody>
</table>

Step 5  Click Save.

The intermediate node is created in the hierarchy.

What to Do Next

Define a local administrator for the intermediate node.

Then create nodes underneath the intermediate node that the intermediate node local administrator can manage.

Delete a Hierarchy Node

Caution

Unintentionally deleting a node can have catastrophic effects on the system. Proceed with caution.

Use this procedure to delete a provider, reseller, customer, site, or intermediate node.

Deleting a provider, reseller, customer, site, or intermediate node results in multiple related items also being deleted. Groups of items are displayed in the order that they must be deleted due to dependencies, and you can delete specific items by group. Checking a group will delete it and all of the groups above it.

Troubleshooting: Errors may occur in the following scenarios:

- Import for a device is running at the time of delete, which may have potential information on the node being deleted (Cisco Unified Communications Manager, CUCxn, or LDAP devices). Cancel all imports before attempting a node deletion.

- A customized data-model was added to the node that is not supported by node deletion. The transaction error should reveal the unsupported data-model. Remove the customized data-model before attempting the node deletion again.

Procedure

Step 1  Login as a provider, reseller, customer, or hcsadmin administrator that can manage the node to be deleted.

Step 2  Select the appropriate node to be deleted:

a) To delete a provider node, select Provider Management > Delete Provider

b) To delete a reseller node, select Reseller Management > Delete Reseller
c) To delete a customer node, select **Customer Management > Delete Customer**
d) To delete a site node, select **Site Management > Delete Site**
e) To delete an intermediate node, select **Hierarchy Management > Delete Intermediate Node**

**Step 3** Select the node to be deleted from the **Node** drop-down list.

**Step 4** To delete the node and all the items dependent on it, check the node. To delete node-specific items by group, click one of the groups above the node.

**Step 5** To perform the deletion, click **Save**.

**Important** There is no confirmation box confirming the delete. Clicking **Save** starts the delete process.

---

### Manage Local Administrators and Operators

Default local Cisco Unified Communications Domain Manager 10.6(1) administrators are created when provider, reseller, customer, and site hierarchy nodes are established. Use this procedure to modify or create additional local administrators or operators. Also use this procedure to create administrators for intermediate nodes.

An administrator for a particular hierarchy level can create or modify the administrators and operators at that hierarchy level and any level below. For example, a Customer XYZ administrator can create other Customer XYZ administrators as well as site administrators for Customer XYZ.

**Procedure**

**Step 1** Log in as an administrator.

**Step 2** To create or modify an admin or operator at a level below your current level, set the hierarchy path at the top of the window.

For example, if you have logged in as provider admin, and want to create a customer admin, set the hierarchy path to the customer for which you want to create the admin.

**Step 3** Select **User Management > Local Admins**.

**Step 4** At a minimum, complete the following fields:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Login username. This field is mandatory.</td>
</tr>
<tr>
<td>Email Address</td>
<td>User email address. This field is mandatory.</td>
</tr>
<tr>
<td>Password</td>
<td>Set the password. This field is mandatory.</td>
</tr>
</tbody>
</table>

**Step 5** To modify an existing administrator or operator, click the administrator or operator.

a) Modify the appropriate settings for the admin or operator.

b) Click **Save**.
Set Localization Language at Hierarchy Node

A default language can be set at any hierarchy node. Users and local administrators will inherit the default language from the nearest hierarchy node in the hierarchy tree that has a default language set. If no default language is specified, English is used. The default language can be overridden for an individual user or local administrator under User Management.

Procedure

Step 1  Log in as provider, reseller, customer, or site admin.
Step 2  Set the hierarchy path to point to the node where you want to set a default language.
Step 3  Select Hierarchy Management > Localization Language.
Step 4  Click Add.
Step 5  Select the default language from the pull down menu.
Step 6  Click Save.

As an example, a provider has not set a default language at the provider level. The provider has a reseller in Germany, so the default language at the reseller is German. But that reseller has a customer in France, so the default language at that customer level is set to French. In addition, the customer in France has a site in Italy, so the default language for that site is set to Italian. In this scenario, users that are not under the reseller will have English as their language by default.
CHAPTER 3

Device Management

- Create the HCM-F Device, page 13
- Cisco Unified Communications Manager Configuration in Cisco Unified CDM, page 15
- Set up Cisco Unity Connection, page 23
- Set up Cisco Emergency Responder, page 25
- Set up Cisco WebEx, page 27
- Set up Customer Equipment, page 28
- Prime Collaboration Assurance Integration with Cisco Unified Communications Domain Manager 10.6(1), page 29
- Enable a Scheduled Data Sync, page 30
- Manually Run the Default Data Sync, page 31
- Controlling a Data Sync with a Model Type List, page 31

Create the HCM-F Device

When you create the HCM-F device, a data sync begins if there is a network connection and the NBI REST service is running on the HCM-F server.

Before You Begin

- Install and configure HCM-F. For more information, see Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1).
- Verify that the NBI REST SDR Web Service is running:
  1. Log in to HCM-F CLI as user admin.
  2. Run the `utils service list` command. Verify that the Cisco HCS NBI REST SDR Web Service is running.
  3. If not running, start it with the `utils service start Cisco HCS NBI REST SDR Web Service` command.
Procedure

Step 1  Log into Cisco Unified Communications Domain Manager 10.x as hcsadmin@sys.hcs.

Step 2  Create a new HCM-F instance:
   a) Select Device Management > HCM-F and click Add.
   b) Enter the HCM-F Host Name.
   c) Enter the HCM-F Admin Username.
   d) Enter the HCM-F Admin Password.
   e) Select the HCM-F Version from the drop-down list.
      Note  Once HCM-F Version is set to a new version, it cannot be changed to an older one.
   f) Click Save.

Step 3  If the previous step fails:
   • Verify HCM-F Hostname is correct
   • Verify HCM-F Admin Username and Admin Password are correct
   • Verify HCM-F Version is correct
   • Verify the domain is set correctly via the Cisco Unified Communications Domain Manager 10.6(1) CLI:
     1  ssh platform@<cucdm hostname>
     2  network domain

Step 4  After a couple of minutes, verify that the initial sync between Cisco Unified Communications Domain Manager and HCM-F is successful:
   a) Select Provider Management > Advanced > SDR Service Provider.
   b) The sync is successful if the default entry, “ServiceProviderName”, appears.

What to Do Next

If the initial sync is still not working after following the above steps, verify the HCM-F REST API is working by browsing to the following URL:
http://<hcmf_app_node_host>/sdr/rest/<hcmf_version>/entity/ServiceProvider.
This should return the JSON representation of the pre-defined ServiceProvider instance in the HCM-F Shared Data Repository (SDR). If you get an error, log in as admin on the HCM-F app node CLI and verify the REST service is running:

To display the services, run the command:  utils service list.
In the output, you should see Cisco HCS NBI REST SDR Web Service[STARTED].
If this service is not started, start it with the command:  utils service start Cisco HCS NBI REST SDR Web Service
For data sync failures, try importing the new HCM-F:

1  Select Device Management > HCM-F and click on the HMC-F device.
2  Update the Hostname and click Save.
3 Import the new HCM-F:
   a Select Device Management > Advanced > Perform Actions.
   b In the Action field, select Import.
   c In the Device field select the HCM-F server.
   d Click Save and wait a few minutes.

4 Check the provider under Provider Management > Advanced > SDR Service Provider.

Cisco Unified Communications Manager Configuration in Cisco Unified CDM

Overview
Cisco Unified Communications Manager devices provide the core call processing capabilities for HCS, and are a critical part of the Cisco Unified Communications Domain Manager provisioning workflows. Cisco Unified Communications Manager devices must be configured before dial plan, user, subscriber, line, and phone configuration can be completed.

Cisco Unified Communications Manager devices can be dedicated to a specific customer, or they can be shared between multiple customers. Cisco Unified Communications Manager devices must then be assigned to one or more Network Device Lists (NDLs), and the NDL is then assigned to one or more sites. The NDL is used to select which Cisco Unified Communications Manager is used for configuration based on the site selected in the hierarchy context.

Shared versus Dedicated
To share the Cisco Unified Communications Manager across multiple customers, add the Cisco Unified Communications Manager at the Provider or Reseller level. To dedicate the Cisco Unified Communications Manager to a single customer, add the Cisco Unified Communications Manager at the Customer level.

When setting up Cisco Unified Communications Manager as a dedicated instance, you can opt to set up Cisco Unified Communications Manager after you create the customer.

Servers within a Cisco Unified Communications Manager Cluster
Within a Cisco Unified Communications Manager cluster, you can configure the following nodes:

- Cisco Unified Communications Manager Publisher
- Cisco Unified Communications Manager Subscriber
- IM and Presence Service Publisher
- IM and Presence Service Subscriber

You must configure a Cisco Unified Communications Manager Publisher node before configuring any other type node.

You must configure an IM and Presence Service Publisher node before configuring an IM and Presence Service Subscriber node.

Synchronization with Cisco Unified Communications Domain Manager 10.6(1)
Set up Cisco Unified Communications Manager Servers

Use this procedure to configure Unified CM servers within a Cisco Unified Communications Manager cluster.

Procedure

**Step 1** Log in as the appropriate hierarchy administrator. Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.

**Step 2** Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.

**Step 3** Click **Device Management > CUCM > Servers**.

**Step 4** Click **Add**.

**Step 5** Enter the Cisco Unified Communications Manager server name in the CUCM Server Name field.

**Note** A Cisco Unified Communications Manager server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to CUCDM** checkbox is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

**Step 6** Select **Voice/Video** in the Server Type field.

**Step 7** To configure a publisher node, check **Publisher**. On the **Publisher** tab, you can specify the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Collab</td>
<td>Select the Prime Collaboration management application monitoring this cluster.</td>
</tr>
<tr>
<td>Call Processing ID</td>
<td>The Call Processing ID of this cluster</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Cluster ID | The Cluster ID of this cluster.
Multi-Tenant | Read-only field. If creating at provider level, this field is set to Shared. If creating at customer level, this field is set to Dedicated.
Version | Select the version of the Cisco Unified Communications Manager Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.
Port | The port on the Cisco Unified Communications Manager server to connect to. Default is 8443.
User Move Mode | Set to Automatic to apply Move Filters when users are synced from Cisco Unified Communications Manager. Set to Manual if you want an Administrator to manually move synced in users to a Site.
User Entitlement Profile | Select the Entitlement Profile that specifies which devices and services users synced from this Cisco Unified Communications Manager are entitled to.

**Note** A violation of the Entitlement Profile does not prevent a user from being synced to Cisco Unified Communications Domain Manager 10.6(1) from Cisco Unified Communications Manager. However, subsequent updates to the user will fail until the user's configuration satisfies the restrictions set in the Entitlement Profile.

**Step 8** For a Unified CM Publisher node, fill in the **Cluster Name** field with the name you want for this cluster. A new cluster is created with this name. This field is required. For Unified CM Subscribers, select the Cisco Unified Communications Manager cluster from the **Cluster Name** drop down menu.

**Step 9** Expand **Network Addresses**.
   a) Select the SERVICE_PROVIDER_SPACE address space.
   b) The Hostname field is automatically populated with the Cisco Unified Communications Manager Server Name. Edit it if necessary.
   c) Enter the IP address of the Cisco Unified Communications Manager Server in the IPV4 Address field.
   **Note** Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Cisco Unified Communications Domain Manager cannot validate an entry that contains a blank space at the end of the hostname or IP address.
   d) Fill in the domain of the Cisco Unified Communications Manager application.
   e) Provide an optional description for the network address.
   If NAT is used, also configure an APPLICATION_SPACE network address.

**Step 10** Expand **Credentials**.
   a) Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
   b) Fill in the user ID and password that you configured when you installed the Cisco Unified Communications Manager.
   c) Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
   d) Provide an optional description for the credential.
ADMIN, HTTP, PLATFORM, and SNMP are required for PCA to manage Cisco Unified Communications Manager. PLATFORM and ADMIN are also required for Service Inventory to generate reports for UC applications.

**Step 11** Click **Save**.
A Cisco Unified Communications Manager network device is created in Cisco Unified Communications Domain Manager 10.6(1). A cluster and Cisco Unified Communications Manager are created in the SDR.

**Step 12** Test the connection between Cisco Unified Communications Manager and Cisco Unified Communications Domain Manager 10.6(1)
- Select **Device Management > Advanced > CUCM Network Device**.
- Click the Cisco Unified Communications Manager you just added.
- Select **Action > Test Connection**.
If the test fails, and you used a hostname, make sure Cisco Unified Communications Domain Manager 10.6(1) has the correct DNS and Domain set.

1. Log in to the platform CLI.
2. Query the current DNS setting: `network dns`
3. Set the DNS if needed: `network dns <dns_server_ip_address>`
4. Query the current domain setting: `network domain`
5. Set the domain if needed: `network domain <domain>`

**Note** Use the CUCM Network Device page only for testing the connection. Do not edit Cisco Unified Communications Manager from this page. To change any configuration of the Cisco Unified Communications Manager, edit it from the **Device Management > CUCM > Servers** page in Cisco Unified Communications Domain Manager 10.6(1).

---

### Set up IM and Presence Service Servers

Use this procedure to configure IM and Presence Service servers within a Cisco Unified Communications Manager cluster.

**Procedure**

**Step 1** Log in as the appropriate hierarchy administrator.
Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.

**Step 2** Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.

**Step 3** Click **Device Management > CUCM > Servers**.

**Step 4** Click **Add**.

**Step 5** Enter the IM and Presence Service server name in the CUCM Server Name field.
An IM and Presence Service server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to CUCDM** checkbox is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

**Step 6** Select **IM_P** in the Server Type field.

**Step 7** To configure a publisher node, check **Publisher**.

**Note** The **Publisher** tab is not populated for an IM and Presence Service publisher node.

**Step 8** Select the Cisco Unified Communications Manager cluster from the **Cluster Name** drop down menu.

**Step 9** Expand **Network Addresses**.

a) Select the SERVICE_PROVIDER_SPACE address space.

b) The Hostname field is automatically populated with the IM and Presence Service Server Name. Edit it if necessary.

c) Enter the IP address of the IM and Presence Service server in the IPV4 Address field.

**Note** Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Cisco Unified Communications Domain Manager 10.6(1) cannot validate an entry that contains a blank space at the end of the hostname or IP address.

d) Fill in the domain of the IM and Presence Service application.

e) Provide an optional description for the network address.

If NAT is used, also configure an APPLICATION_SPACE network address.

**Step 10** Expand **Credentials**.

a) Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.

b) Fill in the user ID and password that you configured when you installed the IM and Presence Service.

c) Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.

d) Provide an optional description for the credential.

**Note** ADMIN, HTTP, PLATFORM, and SNMP are required for PCA to manage IM & Presence Service. PLATFORM and ADMIN are also required for Service Inventory to generate reports for UC applications.

**Step 11** Click **Save**.

---

**CUP Cluster Migration**

In versions before Cisco Unified Communications Domain Manager 10.6(1), IM and Presence Service (previously known as CUP) was set up in a cluster separate from the Cisco Unified Communications Manager cluster. This configuration is called a multi-cluster configuration. Beginning with Unified CDM 10.6(1), however, the IM and Presence Service servers are set up as part of the Cisco Unified Communications Manager cluster itself, in what is called a single-cluster configuration. The single-cluster configuration correctly represents the Cisco Unified Communications Manager cluster with its IM and Presence Service servers in the management layer. This configuration eliminates the confusion that multi-cluster configurations can cause
for administrators when Cisco Prime Collaboration Assurance and other tools show these servers in different clusters.

Figure 1: Multi-Cluster vs. Single Cluster Configuration

Although the use of multi-cluster configurations is deprecated and highly discouraged, Unified CDM 10.6(1) continues to support multi-cluster configurations for backward compatibility and upgrades. Partners are strongly encouraged to use the single-cluster configuration for new clusters. Convert existing multi-cluster configurations to single-cluster using the migration tool under Device Management.

Migrate CUP to a Cisco Unified Communications Manager Cluster

Use this tool to migrate your CUP (also known as IM and Presence Service) nodes to a Cisco Unified Communications Manager cluster, which is the recommended configuration. Migrating CUP nodes to a Cisco Unified Communications Manager cluster is hierarchy specific; i.e., a Customer CUP node can only be migrated to a Customer Cisco Unified Communications Manager cluster and not to a Provider or Reseller cluster. A Publisher IM_P node is added first, then Subscriber nodes.

When migrating your CUP to a Cisco Unified Communications Manager cluster, the following conditions apply:

• Cluster versions should be same for both the clusters.
• The IPV4 address or hostname and domain configuration should not be duplicated within the cluster.
• Two devices cannot have the same server name.
• No more than one CUP publisher can be migrated to the same Cisco Unified Communications Manager cluster.
• Multiple subscribers can be migrated to the same Cisco Unified Communications Manager cluster.

Procedure

Step 1 Login as a provider, reseller, or customer admin, depending on the hierarchy level where the CUP cluster was configured.
Step 2 Set the hierarchy path to the hierarchy node where the CUP cluster was configured. For a shared configuration, this would be a provider or reseller node. For a dedicated configuration, this would be a customer node.
Step 3 Click Device Management > CUP (deprecated) > Migrate CUP to CUCM Cluster.
Step 4 In the From CUP Cluster pull-down menu, click and select the CUP cluster you want to migrate.
Step 5 In the To CUCM Cluster pull-down menu, click and select the Cisco Unified Communications Manager cluster to which you want to migrate the CUP cluster.
Step 6 Click Save.

The migrated CUP server is removed from the list under Device Management > CUP > Servers and now appears under Device Management > CUCM > Servers as server type IM_P. The cluster name for these migrated servers is now the same as the Cisco Unified Communications Manager cluster name.

Cisco Unified Communications Manager Server Deletion

Be aware that deleting a Cisco Unified Communications Manager Server in Cisco Unified Communications Domain Manager 10.6(1) will also delete local data that has been synced to it from the Cisco Unified Communications Manager Server, including:

• Users
• Dial Plan information
• Configuration parameters

Configure Regions

Regions can only be added at the customer or site hierarchy level but can be modified at any hierarchy level. Regions added directly on Cisco Unified Communications Manager are synced in at the hierarchy level the Cisco Unified Communications Manager is configured at in Cisco Unified Communications Domain Manager 10.6(1).
**Procedure**

**Step 1** Log in as the Provider/Reseller or Customer administrator.

**Step 2** Select **Device Management > CUCM > Regions** from the left menu.

**Step 3** Perform one of the following:
- To add a new Region, click **Add**.
- To edit an existing Region, click on the name of the Region to be updated.

**Step 4** From the **CUCM** pulldown menu, select or modify the Cisco Unified Communications Manager that corresponds to the Region.

**Step 5** Enter a unique name for the new Region in the **Name** field, or modify the existing **Name** if desired.

**Step 6** In the **Related Regions** field, configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region Name</td>
<td>Drop down menu with list of available regions. This field is mandatory.</td>
</tr>
<tr>
<td>Codec Preference</td>
<td>This is a drop-down containing available Audio Codec Preference Lists. The default codec is G.711.</td>
</tr>
<tr>
<td>Audio Bandwidth</td>
<td>Maximum Audio Bit Rate (kbps). This field is mandatory.</td>
</tr>
<tr>
<td>Video Bandwidth</td>
<td>Maximum Session Bit Rate for Video Calls (kbps). This field is mandatory.</td>
</tr>
<tr>
<td>Immersive Video Bandwidth</td>
<td>Maximum Session Bit Rate for Immersive Video Calls (kbps). This field is mandatory.</td>
</tr>
</tbody>
</table>

**Step 7** To save a new or updated group, click **Save**.

---

**Delete Region**

Regions can be deleted at any hierarchy level. Related regions cannot be removed from a region. They exist until either region is deleted.

**Procedure**

**Step 1** Log in as the Provider/Reseller or Customer administrator.

**Step 2** Select **Device Management > CUCM > Regions** from the left menu.

**Step 3** From the list of Regions, click on the name of the Region to be deleted.

**Step 4** Click **Delete**.

**Step 5** From the popup window, click **Yes** to confirm the deletion.
Set up Cisco Unity Connection

Overview
Cisco Unity Connection devices provide voicemail services for HCS deployments, and can be dedicated to a customer or shared across multiple customers. To dedicate a Cisco Unity Connection to a single customer, configure the Cisco Unity Connection at the customer hierarchy node. To share a Cisco Unity Connection across multiple customers, configure the Cisco Unity Connection at a hierarchy node above the customer (reseller, provider, or intermediate node). The Cisco Unity Connection device must be included in one or more Network Device Lists (NDLs), and the NDL must be assigned to one or more sites.

Synchronization with Cisco Unified Communications Domain Manager 10.6(1)
Configuring a Cisco Unity Connection device on Cisco Unified Communications Domain Manager 10.6(1), creates a scheduled data sync to import model data from the device into Cisco Unified Communications Domain Manager 10.6(1). The scheduled data sync ensures that the Cisco Unified Communications Domain Manager 10.6(1) cache maintains the most current view of the configured device. Any changes to the configuration occurring on the device, including additions, deletions, or modifications, will be reflected in Cisco Unified Communications Domain Manager 10.6(1) after the next data sync.

The data sync occurs once immediately upon creation. The recurring sync is scheduled to occur every 14 days, but is disabled by default. You can enable the sync and modify the schedule from Device Management > CUC > Schedules. When determining the appropriate schedule setting, the frequency of the sync must be weighed against the additional processing and network activity associated with the data sync. You can also manually run the data sync at any time from Device Management > Advanced > Perform Publisher Actions, or from Administration Tools > Data Sync.

The performance of a data sync can be improved by controlling the types of data that are synced. See Controlling a Data Sync with a Model Type List, on page 31 for more information.

Procedure

Step 1 Log in as the appropriate hierarchy administrator.
Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.

Step 2 Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.

Step 3 Click Device Management > CUC > Servers.

Step 4 Click Add.

Step 5 Enter a Cisco Unity Connection server name in the CUC Server Name field.
Note A Cisco Unity Connection server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager 10.6(1) may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the Migrate from HCM-F to CUCDM checkbox is displayed. Click Save to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

Step 6 Check Publisher if you are configuring a publisher node.
Note The Publisher tab is populated only when the Publisher check box is checked.
On the Publisher tab, you can specify the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Collab</td>
<td>Select the Prime Collaboration management application monitoring this cluster.</td>
</tr>
<tr>
<td>Call Processing ID</td>
<td>The Call Processing ID of this cluster</td>
</tr>
<tr>
<td>Cluster ID</td>
<td>The Cluster ID of this cluster.</td>
</tr>
<tr>
<td>Multi-Tenant</td>
<td>If creating at provider level, this field is read only and set to Shared. If creating at customer level, you can choose between Dedicated and Partitioned.</td>
</tr>
<tr>
<td>Version</td>
<td>Select the version of Cisco Unity Connection Servers in this cluster. The available versions depend on the version of HCM-F that has been configured.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on the Cisco Unity Connection server to connect to. Default is 8443.</td>
</tr>
</tbody>
</table>

**Step 7** Fill in the Cluster Name field with the name you want for this cluster. A new cluster is created with this name. This field is mandatory.

**Note** If Publisher is not checked, the Cluster field appears as a drop-down list where you select an existing cluster.

**Step 8** Expand **Network Addresses**.

a) Select the SERVICE_PROVIDER_SPACE address space.
b) The Hostname field is automatically populated with the Cisco Unity Connection Server Name. Edit it if necessary.
c) Enter the IP address of the Cisco Unity Connection Server in the IPV4 Address field.
   **Note** Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Cisco Unified Communications Domain Manager 10.6(1) cannot validate an entry that contains a blank space at the end of the hostname or IP address.
d) Fill in the domain of the Cisco Unity Connection application.
e) Provide an optional description for the network address.

If NAT is used, also configure an APPLICATION_SPACE network address.

**Step 9** Expand **Credentials**.

a) Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
b) Fill in the user ID and password that you configured when you installed the Cisco Unity Connection.
c) Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
d) Provide an optional description for the credential.

ADMIN, HTTP, and SNMP are required for PCA to manage Cisco Unity Connection. PLATFORM and ADMIN are required for Service Inventory to generate reports for UC applications.

**Step 10** Click **Save**.
Cisco Unity Connection Server Deletion

Be aware that deleting a Cisco Unity Connection Server in Cisco Unified Communications Domain Manager 10.6(1) also deletes local data that has been synced to it from the Cisco Unity Connection Server, including:

- Users
- Dial Plan information
- Configuration parameters

Set up Cisco Emergency Responder

Complete this procedure at any time to configure Cisco Emergency Responder (CER) on Cisco Unified Communications Domain Manager 10.6(1). For more information on CER installation and setup, refer to http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cer/10_5_1/english/administration/guide/CER0_BK_C0C71A60_00_cisco-emergency-responder-administration-guide.html.

Procedure

Step 1 Log in as the appropriate hierarchy administrator.

Step 2 Set the hierarchy path to the correct level. Shared instances are created at the Provider, Reseller, or Customer level. Dedicated instances are created at the customer level.

Step 3 Click Device Management > CER > Servers.

Step 4 Perform one of the following:

- To add a new Cisco Emergency Responder (CER) in Cisco Unified Communications Domain Manager 10.6(1), click Add.
- To modify an existing CER, click its name in the list of Cisco Emergency Responders.

Step 5 Enter a name for the Cisco Emergency Responder in the CER_Virtual Server Name Field.

Note A Cisco Emergency Responder server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the Migrate from HCM-F to CUCDM checkbox is displayed. Click Save to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

Step 6 Check Publisher if you are configuring a publisher node.

Note The Publisher tab is populated only when the Published check box is checked.

Step 7 Expand Network Addresses.

a) Select the SERVICE_PROVIDER_SPACE address space.

b) Enter the IP address of the CER Server in the IPV4 Address field.

Note Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Cisco Unified Communications Domain Manager 10.6(1) cannot validate an entry that contains a blank space at the end of the hostname or IP address.

c) The Hostname field is automatically populated with the CER Name. Edit it if necessary.
d) Fill in the domain of the CER application.
e) Provide an optional description for the network address.

**Step 8**  
Expand **Credentials**.

a) Add credentials for PLATFORM and ADMIN credential types. Click + to add more credentials.
b) Fill in the user ID and password that you configured when you installed the CER.
c) Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
d) Provide an optional description for the credential.

PLATFORM and ADMIN are required for license management.

**Step 9**  
On the **Publisher** tab, you can specify the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td>Select the version of the Cisco Emergency Responder Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.</td>
</tr>
<tr>
<td><strong>Multi-Tenant</strong></td>
<td>Read-only field. If creating at provider level, this field is set to Shared. If creating at customer level, this field is set to Dedicated.</td>
</tr>
</tbody>
</table>

**Step 10**  
Click Save.

---

**What to Do Next**

*Associate CER with Customers*, on page 26

---

**Associate CER with Customers**

**Before You Begin**

A customer must be configured before performing this procedure. Perform this procedure at any hierarchy level at or above where the CER is configured, when you configure the VM in Cisco Unified Communications Domain Manager 10.6(1), or perform it at any time after the VM has been created.

**Procedure**

**Step 1**  
Log in as a Provider or Reseller administrator.

**Step 2**  
Select **Device Management > CER > Servers**.

**Step 3**  
Click the name of the CER cluster to associate with a customer.

**Step 4**  
Click the **CustomerAssociation** tab.

**Note**  
The list of customers that appear on this tab are those at, and below your current hierarchy. For example, if you are at the Provider level, and the CER is at Reseller1, you can see all customers at the Provider level and below. An error will occur if you try to associate a customer out of the CER’s scope.

**Step 5**  
Check the box to the left of each customer to be associated with the CER cluster.
View Associated Clusters on CER Servers

Before You Begin
Customers must be associated with the Cisco Emergency Responder (CER) cluster in order to be viewed in this procedure, unless the CER is created at customer level. If the CER is created at the customer level, customer information is automatically filled in for the customer where the CER exists.

Procedure

Step 1 Log in as a Provider, Reseller, or Customer administrator.
Step 2 Make sure that the hierarchy is set to the customer you wish to view.
Step 3 Select Device Management > CER > Servers.
Step 4 Click the name of the CER cluster to be viewed.
Information appears about the CER cluster. You can view a list of customers associated with the CER server by selecting the Customer Association tab.

Set up Cisco WebEx

For additional information about conferencing, see Cisco Hosted Collaboration Solution, Release 10.6(1) End-User Provisioning Guide.

Procedure

Step 1 Log in as a provider or reseller administrator.
Step 2 Select Device Management > WebEx > Servers.
Step 3 Click Add.
Step 4 Complete the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>WebEx server type. Read-only field set to Cloud-Based.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used to communicate with WebEx server. This field is mandatory and defaults to https.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address or hostname of the WebEx server. This field is mandatory. Example: site-name.webex.com</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>The port used to communicate with the WebEx Server. Defaults to 443.</td>
</tr>
<tr>
<td>Site Name</td>
<td>The name of the site to be managed. Usually matches the start of the WebEx</td>
</tr>
<tr>
<td></td>
<td>address.</td>
</tr>
<tr>
<td>Site Id</td>
<td>An ID for the site being managed. Typically received from Cisco WebEx Site</td>
</tr>
<tr>
<td></td>
<td>Provisioning group. Provide this field before testing the connection to the</td>
</tr>
<tr>
<td></td>
<td>WebEx server.</td>
</tr>
<tr>
<td>Partner Id</td>
<td>Partner ID. Typically received from Cisco WebEx Site Provisioning group.</td>
</tr>
<tr>
<td>REST URI</td>
<td>The relative URI for the XML service on the WebEx server. This field is</td>
</tr>
<tr>
<td></td>
<td>mandatory and defaults to WBXService/XMLService.</td>
</tr>
<tr>
<td>WebEx Id</td>
<td>WebEx administrator ID. Either the WebEX Id or the Email field is mandatory.</td>
</tr>
<tr>
<td>Email</td>
<td>Email address of WebEx administrator. Either the WebEX Id or the Email field</td>
</tr>
<tr>
<td></td>
<td>is mandatory.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the provided WebEx administrator. This field is mandatory.</td>
</tr>
<tr>
<td>Repeat Password</td>
<td>Confirm password for the provided WebEx administrator. This field is</td>
</tr>
<tr>
<td></td>
<td>mandatory.</td>
</tr>
<tr>
<td>Version</td>
<td>Supported WebEx version.</td>
</tr>
</tbody>
</table>

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

**What to Do Next**

To test the connection to the WebEx server, select **Device Management** > **Advanced** > **WebEx Network Device**. Click the WebEx server, then select **Action** > **Test Connection**.

**Set up Customer Equipment**

Use this procedure to associate customer equipment with the Prime Collaboration application that monitors it.

**Procedure**

**Step 1**  Log in as a Customer or Site administrator.
**Step 2**  Set the hierarchy path to the appropriate site.
**Step 3**  In the left menu, select **Device Management** > **Customer Equipment**.
**Step 4**  Click **Add**. The following fields appear:
The only required fields are Customer Equipment Name, at least one network address, and one credential if associating Prime Collaboration. Ensure that the network address does not contain a trailing blank space. Cisco Unified Communications Domain Manager 10.6(1) cannot validate an entry that contains a blank space at the end of the hostname or IP address.

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

---

**Prime Collaboration Assurance Integration with Cisco Unified Communications Domain Manager 10.6(1)**

To enable integration between Cisco Unified Communications Domain Manager 10.6(1) and Prime Collaboration Assurance use the following workflow:

1. Synchronize your customer information with Cisco Unified Communications Domain Manager 10.6(1).
2. Add the local IP address of your Cisco Unity Connection and Cisco IM and Presence Service to Cisco Unified Communications Domain Manager 10.6(1). This ensures that your Prime Collaboration Assurance server has the Private IP Address.
3. Add IM and Presence Service sub node information to Cisco Unified Communications Domain Manager 10.6(1) if the customer has multiple instances of IM and Presence deployed.
4. Ensure that your Unified Communication applications have all needed credentials. At the minimum, you need to have credentials for Administration, platform, SNMP, and HTTP.

**Note**  Depending on what you need to monitor, additional credentials may be needed. For more information about required protocols/support and credentials needed to set up devices for Prime Collaboration Assurance monitoring see **Setting up devices for Prime Collaboration Assurance**.

5. Ensure that your CUBE_SP and CPE have required credentials (SNMP and CLI).
6. Add Prime Collaboration Assurance to Cisco Unified Communications Domain Manager 10.6(1) under **Device Management > Prime Collab > Servers**. (Administration and SFTP credentials are needed.)
7 On-board the customer to Prime Collaboration Assurance using the Cisco Unified Communications Domain Manager 10.6(1) Admin GUI. CHPA will push SNMP/Syslog/Billing server configuration information to your Cisco Unified Communications Manager automatically. Syslog/SNMP configurations for Cisco Unity Connection and IM and Presence Service have to be added manually prior to on-boarding.

Note

CHPA only supports Cisco Unified Communications Manager in HCS 10.6(1). To ensure successful CHPA configuration, the following credentials need to be configured in the Cisco Unified Communications Manager nodes:

- Administration credentials for Cisco Unified Communications Manager
- Platform credentials for Cisco Unified Communications Manager
- SNMP and HTTP credentials for Unified Communications Manager
- SFTP for Prime Collaboration Assurance

The following configuration will be pushed to Cisco Unified Communications Manager:

- The SNMP community string
- CDR (SFTP of Prime Collaboration Assurance server)
- Syslog configuration

JTAPI credentials are optional credentials used for TelePresence session monitoring. They are used to retrieve session status information from TelePresence devices. You must create a JTAPI user in the Unified Communications Manager with the required permission to receive JTAPI events on endpoints. JTAPI configuration is not supported by CHPA in HCS 10.1(2) and therefore the credentials must be manually configured in the Cisco Unified Communications Manager. Note also that Prime Collaboration Assurance manages multiple call processor clusters and as a result you must ensure that the cluster IDs are unique.

8 Verify the devices are managed in Prime Collaboration Assurance.

Devices supported by Prime Collaboration Assurance can be found at: Supported Devices.

**Enable a Scheduled Data Sync**

By default, when a Cisco Unified Communications Manager or Cisco Unity Connection device is set up in Cisco Unified Communications Domain Manager 10.6(1), a full data sync instance is created to perform the initial sync of all data from the device. In addition, a Schedule is created to execute that data sync every 14 days, but is disabled by default. It is recommended to run the full data sync manually only when necessary. However, if a regularly scheduled sync is desired, the schedule can be enabled as follows:
Procedure

Step 1  Log in as provider admin.
Step 2  Select Administration Tools > Scheduling.
Step 3  Select the schedule instance that matches the following naming convention: HcsSync-<ip_address>-<device_name>-SCHED. For example: HcsSync-192.0.2.24-CUCM01-SCHED
Step 4  Check the Active checkbox.
Step 5  Click the Multiple Executions tab, and update the interval, if desired.
Step 6  Click Save.

The full data sync will execute immediately, and will execute again according to the schedule.

Manually Run the Default Data Sync

You can always manually run the default data sync when there have been updates to Cisco Unified Communications Manager or Cisco Unity Connection devices that need to be synced into Cisco Unified Communications Domain Manager 10.6(1).

Procedure

Step 1  Log in as a provider or reseller admin.
Step 2  Select Device Management > Advanced > Perform Publisher Actions.
Step 3  For Action, select Import.
Step 4  For App Type, select CUCM Device or CUC Device.
Step 5  Select the device from the Available Clusters list and click Select.
Step 6  Click Save.

Controlling a Data Sync with a Model Type List

Using a Model Type List (MTL), you can control the types of data that are synced into Cisco Unified Communications Domain Manager 10.6(1) from Cisco Unified Communications Manager or Cisco Unity Connection devices. Controlling the types of data that are synced can greatly improve sync performance. The MTL is a list of device models associated with the device type, for example, Phone and Line device models that are associated with the Cisco Unified Communications Manager device.

These are the possible types of Model Type Lists:

Include Selected Model Types

This list represents the device models to explicitly include in the data sync.
Exclude Selected Model Types

This list represents the device models to explicitly exclude from the data sync.

Ordered List

This list represents the device models to explicitly include in the data sync in the order they must be synced.

A data sync created with an empty Model Type List attribute results in the subsequent import(s) synchronizing all device models for the corresponding device.

Here's an example of an include MTL:

<table>
<thead>
<tr>
<th>Model Type List [HCS CUCM Media MTL]</th>
<th>Save</th>
<th>Delete</th>
<th>Help</th>
<th>Back</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List Type*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Include Selected Model Types</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model Types</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[device/cucrm/MediaResourceGroup]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[device/cucrm/MediaResourceList]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[device/cucrm/MainServer]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[device/cucrm/MainAudioSource]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[device/cucrm/Mtp]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A data sync using this MTL will sync all Media Resource Group, Media Resource Lists, Music on Hold servers and audio sources, and Media Termination Points. No other data will be synced from Cisco Unified Communications Manager.

It is recommended to define MTLs for sets of data that are being modified on the device directly, particularly Cisco Unified Communications Manager because this is where the bulk of the configuration data for each customer resides. By defining MTLs that target specific data sets rather than doing a full sync, the performance of Cisco Unified Communications Domain Manager 10.6(1) can be maintained with better response times and quicker transaction execution. Some Cisco Unified Communications Manager device models to avoid unless needed are Users, Phones, and Lines, as there may be large numbers of these in the Cisco Unified Communications Manager and result in a lengthy data sync operation.

Data sync overhead can be further reduced if you want to sync only new and deleted instances of the device model and not updates to existing instances. This can be done by unchecking the Refresh Existing Data checkbox on the Data Sync configuration page. This checkbox controls whether existing device model instances are updated in Cisco Unified Communications Domain Manager 10.6(1) in addition to importing new instances and removing deleted instances. If checked, all device model instances must be synced and examined. If unchecked, only new and deleted instances need to be imported and the data sync will run considerably faster.
Create a Targeted Model Type List

If you manage data on Cisco Unified Communications Manager or Cisco Unity Connection directly on a regular basis, perhaps for configuration that is not orchestrated from Cisco Unified Communications Domain Manager 10.6(1) such as media resources, it is recommended to create a Model Type List and Data Sync specifically targeting the data items you are managing. This ensures each data sync is highly optimized for the data being changed on Cisco Unified Communications Manager directly and minimizing the load on Cisco Unified Communications Domain Manager 10.6(1). To create a targeted Model Type List:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in as hcsadmin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Administration Tools &gt; Model Type List.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Specify the name of the Model Type List. It is recommended to use a naming convention that makes it easy to identity the MTL in a list view, such as CUCM Media Resources.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Specify the List Type. Select Include Selected Model Types if the list of device models you want to sync is relatively short. Select Exclude Selected Model Types if the list of device models you want to sync is relatively long. Exclude device models that tend to have lots of instances, like users, phones, and lines. Select Ordered List if the list of device models you want to sync is relatively short and the order in which they are synced matters.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Add Model Types to the list of device models that are to be included or excluded according to the List Type selected. See View List of Device Models, on page 33 for information on how to see a list of available Cisco Unified Communications Manager and Cisco Unity Connection device models.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

View List of Device Models

Use this procedure to see the device models available to use in Model Type Lists for custom data syncs from Cisco Unified Communications Manager or Cisco Unity Connection.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in as hcsadmin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the ? on the menu bar to open Online Help.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Model API.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Device/Cuc or Device/Cucm.</td>
</tr>
</tbody>
</table>
Create a Custom Data Sync

Create a custom data sync to use a targeted Model Type List.

**Procedure**

**Step 1** Log in as hcsadmin.
**Step 2** Select Administration Tools > Data Sync.
**Step 3** Click Add.
**Step 4** Specify the name of the Data Sync. It is recommended to use a naming convention that makes it easy to identify the data syncs in the list view, such as `C1Pull-CUCM01-DS` where C1 is the customer name, Pull is the data sync type, CUCM01 is the name of the Cisco Unified Communications Manager, and DS stands for Data Sync. You could also include the type of data included in the sync, such as `C1Pull-CUCM01-MediaResources-DS`.
**Step 5** For Sync Type, select Pull from Device.
**Step 6** For Dependency Resolution, select Default.
**Step 7** Check Execute Asynchronously and Refresh Existing Data. Execute Asynchronously means that the sync request will return a reply before its complete when executed from the API. Refresh Existing Data means that all instances of the device models specified in the Model Type List will be updated.
**Step 8** Select the targeted Model Type List you defined earlier.
**Step 9** Leave Synchronization Order and Model Instance Filter blank.
**Step 10** Select the Device Type you are syncing from.
**Step 11** Click + on Device Filters to add an entry to the list.
   a) For Attribute Name, select host.
   b) For Condition, select Equals.
   c) For Value, select the hostname/IP address of the device.
**Step 12** Leave Workflows empty.
**Step 13** Click Save.

**What to Do Next**

To run the custom data sync, click the data sync from the Data Sync list and click Execute.
Customer Configuration

- Configure Network Device List, page 35
- Network Device List Selection Rules, page 36

Configure Network Device List

A Network Device List (NDL) is a list of network devices that are assigned to a Site. An NDL can contain one instance each of Cisco HCM-F, Cisco Unified Communications Manager, Cisco Unity Connection, and Cisco WebEx. Only Cisco HCM-F is required.

NDLs can be defined only at the Customer hierarchy level. A customer can have multiple NDLs defined.

NDLs can be defined only by a Provider or Reseller admin.

The HCM-F device is pre-populated in the NDL and should not be changed.

Shared UC Applications (that is, UC Applications that are defined above the Customer hierarchy level) can be included in an NDL. However, to use that NDL, the customer must be defined as allowing Shared UC Applications.

Once an NDL is assigned to any Site, the only supported modifications are:

- Network Device List Name can be changed.
- Network Device List Description can be changed.
- New devices can be added.

An NDL cannot be deleted if it is assigned to any Site.

---

Note

- Unified Communications application clusters are not linked to the customer until the Network Device list has been created.
- Only publisher nodes are shown in the dropdown list for Cisco Unified Communications Manager and Cisco Unity Connection.
Procedure

Step 1  Log in to as a provider admin or reseller admin.
Step 2  Click Customer Management > Network Device Lists. Select a customer on the hierarchy tree where the Network Device List (NDL) is to be created.
Step 3  Click Add.
Step 4  Enter a name for the NDL and optionally a description.
Step 5  Click the + next to Cisco Unified CM.
Step 6  Select the Cisco Unified Communications Manager instance from the dropdown menu.
Step 7  (Optional) Add Cisco Unity Connection and Cisco WebEx instances to the NDL.
Step 8  Click Save.

Network Device List Selection Rules

If an administrator at a hierarchy has access to more than one Network Device List (NDL), the option to choose a specific hardware group or list may be needed in order to provision a set of devices. The Network Device List Reference (NDLR) does not offer such a choice.

The Rule Model Device Selection Type model provides a solution to this problem and instances of it are a set of rules for views and relations at a hierarchy level. A particular NDL can then be selected from a pop-up form before the Add form of these model types are shown. In this way the administrator can then select the specific required NDL.

When an instance of the Rule Model Device Selection Type model is added, the target relation or view is specified and more than one a set rules can be added for it - one for each relevant Hierarchy Node Type.

In addition, a Default GUI Rule that is applied to the Relation or View is reflected as the Default value for the Permitted Hierarchy Node Type.

In addition to this behavior, the following rules apply:

- The NDL popup is only available for Relations and Views.
- Device form fields will be filtered according to the device listed in the selected NDL.
- More than one type of device is supported for the selected NDL.
- Any Provisioning Workflow Network Device Filters (NDF) override a selected NDL device choice.
- Only the Add operation supported.
- NDL popups are controlled by GUI Rules at hierarchy levels for model types. The device selection given GUI Rules, NDLs, NDLRs and Device Selection Rules are shown in the table below.

<table>
<thead>
<tr>
<th>GUI Rule</th>
<th>NDL(s)</th>
<th>NDLR</th>
<th>Use Popup</th>
<th>Use NDLR</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>N</td>
<td>N</td>
<td>*</td>
<td>*</td>
<td>Normal Device selection</td>
</tr>
</tbody>
</table>
The Rule Model Device Selection Type model also provides the following functionality:

- The NDL device meta is available to the context in Provisioning Workflows. For example:

```json
"device_meta": { 
    "ndl": { 
        "name": "NDL1", 
        "pkid": "54dc76c82afa4327de0d218e", 
        "data/CallManager": { 
            "pkid": "54dc76c72afa4327de0d217f", 
            "bkey": "["10.120.2.175", ","8443", ","P.C"]"
        } 
    } 
}
```
• NDL device meta namespace `device_meta` is available in macros as: `{ device_meta.??? }`, for example:

```java
device_meta.ndl.name
device_meta.ndl.data/CallManager.pkid
```

• The `[ndl]` macro is available for use in GUI Rules - similar to `[hierarchy]`.

• An API parameter is available for the selected NDL when a GET request is sent for the Add form of a Relation. The value of `[ndl]` in the example below will be a valid PKID for the NDL. For example:

```bash
GET /api/v0/relation/UswerCucmCucRel/add/?
hierarchy=[hierarchy]&
ndl=[ndl]&
schema=true&
schema_rules=true
```

This parameter will be transformed in the subsequent Add calls to devices to a device parameter.
Site Management

- Create Site, page 39
- Modify Site Defaults, page 40
- Cisco Hosted Collaboration Solution Roles and Privileges, page 44

Create Site

Procedure

**Step 1**  Log in to server as a Provider, Reseller, or Customer admin.

**Step 2**  Make sure that the hierarchy is set to the customer for whom you are creating the site.

**Step 3**  Click *Site Management > Sites*.

**Step 4**  Click *Add*.

**Step 5**  Complete the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>The name of the site. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Any spaces in the site name will be converted to underscores in the site</td>
</tr>
<tr>
<td></td>
<td>local administrator name and e-mail, if Create Local Admin is checked.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the site</td>
</tr>
<tr>
<td>Extended Name</td>
<td>The Extended Name of the site can be used by external clients if needed.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This field exists in the Customer Location record in SDR. When the customer</td>
</tr>
<tr>
<td></td>
<td>is managed by Cisco Unified Communications Domain Manager 8.1(x), the</td>
</tr>
<tr>
<td></td>
<td>Extended Name is synced from Cisco Unified Communications Domain Manager</td>
</tr>
<tr>
<td></td>
<td>8.1(x) to the Customer Location record in SDR. When the customer is</td>
</tr>
<tr>
<td></td>
<td>managed by Cisco Unified Communications Manager 10.x, the Extended Name</td>
</tr>
<tr>
<td></td>
<td>is synced from Cisco Unified Communications Manager 10.x to the Customer</td>
</tr>
<tr>
<td></td>
<td>Location record in SDR.</td>
</tr>
</tbody>
</table>
### Modify Site Defaults

Site defaults provide the default values for many tasks undertaken while onboarding, and are not limited to the Subscriber Management tasks. When a site is created, a site defaults instance is created on that site with the same name as the site. Many of the attributes in this data model are NOT directly related to dial plan and contain default values when this instance is created. When a Cisco HCS site dial plan is created, the site defaults on that site is updated. The items that are updated are dial plan-related attributes that are affected by the site dial plan that was deployed. If these specific site defaults attributes already had values before the site dial plan was deployed, they are overwritten. When the site dial plan is removed, these same attributes will be reset (set to empty string) in the site defaults.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External ID</td>
<td>The External ID of the site can be used by external clients if needed. This field is not used by other components within Cisco HCS.</td>
</tr>
<tr>
<td>Create Local Admin</td>
<td>Controls whether a default local administrator is created for the site.</td>
</tr>
<tr>
<td>Cloned Admin Role</td>
<td>The customer role used to create a new role prefixed with the site name. The created site role, shown in <strong>Default Admin Role</strong> field, is assigned to the default local admin user. This field appears only if <strong>Create Local Admin</strong> is checked.</td>
</tr>
<tr>
<td>Default Admin Role</td>
<td>The created site role that is assigned to the default local admin. This field is read only and appears only if <strong>Create Local Admin</strong> is checked.</td>
</tr>
<tr>
<td>Default Admin Password</td>
<td>The password to assign to the default local admin. This field appears only if <strong>Create Local Admin</strong> is checked.</td>
</tr>
<tr>
<td>Repeat Default Admin Password</td>
<td>Confirm the default local admin password. This field appears only if <strong>Create Local Admin</strong> is checked.</td>
</tr>
<tr>
<td>Country</td>
<td>The country is used to determine which dial plan to download to the site when the dial plan is configured on the site. This field is mandatory.</td>
</tr>
<tr>
<td>Network Device List</td>
<td>Choose the NDL containing the UC applications and WebEx to be used by the site. Once an NDL has been set for the site, it cannot be removed from the site, nor can the NDL be changed to another NDL.</td>
</tr>
</tbody>
</table>

**Step 6** Click **Save**.

Once saved, the following occurs:

- A Site hierarchy node is created
- A Location in is created
- A CustomerLocation in the SDR is created
- Optionally, a default site admin is created

---

### Modify Site Defaults

Site defaults provide the default values for many tasks undertaken while onboarding, and are not limited to the Subscriber Management tasks. When a site is created, a site defaults instance is created on that site with the same name as the site. Many of the attributes in this data model are NOT directly related to dial plan and contain default values when this instance is created. When a Cisco HCS site dial plan is created, the site defaults on that site is updated. The items that are updated are dial plan-related attributes that are affected by the site dial plan that was deployed. If these specific site defaults attributes already had values before the site dial plan was deployed, they are overwritten. When the site dial plan is removed, these same attributes will be reset (set to empty string) in the site defaults.
Procedure

**Step 1** Log in to server as a Provider, Reseller, or Customer admin. For a list of the roles and tasks that can be done at each level, see Cisco Hosted Collaboration Solution Roles and Privileges, on page 44.

**Step 2** Select an available site from the hierarchy node breadcrumb at the top of the view.

**Step 3** Select Site Management > Defaults.

**Step 4** From the General Defaults tab, click the following fields to modify their default values as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Site name</td>
</tr>
<tr>
<td></td>
<td>This field is mandatory. It should be the same name as the site. Only one instance of site defaults exist for a site.</td>
</tr>
<tr>
<td>Default CUCM Device Pool</td>
<td>Default value: Cu{CustomerId}Si{SiteId}-DevicePool</td>
</tr>
<tr>
<td>Default CUCM Location</td>
<td>Default value: Cu{CustomerId}Si{SiteId}-Location</td>
</tr>
<tr>
<td>Default User Profile</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Default CUCM MeetMe Partition</td>
<td>Default value: Cu{CustomerId}Si{SiteId}-Feature-PT</td>
</tr>
<tr>
<td>Default CUCM Call Pickup Partition</td>
<td>Default value: Cu{CustomerId}Si{SiteId}-Feature-PT</td>
</tr>
<tr>
<td>Default CUCM Group</td>
<td>Default value: Default</td>
</tr>
<tr>
<td>Default CUCM Call Park Partition</td>
<td>Default value: Cu{CustomerId}Si{SiteId}-Feature-PT</td>
</tr>
<tr>
<td>Default CUCM Hunt Pilot Partition</td>
<td>Default value: Cu{CustomerId}Si{SiteId}-Feature-PT</td>
</tr>
</tbody>
</table>

**Step 5** From the Device Defaults tab, click the following fields to modify their default values as required. These default values are applied to the configuration template associated with adding a subscriber (SubscriberPhonePrePopulate).

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default CUCM Device Profile Product</td>
<td>Default value: Cisco 9971</td>
</tr>
<tr>
<td>Default CUCM Device Profile Protocol</td>
<td>Default value: SIP</td>
</tr>
<tr>
<td>Default CUCM Device Profile Button Template</td>
<td>Default value: Standard 9971 SIP</td>
</tr>
<tr>
<td>Default CUCM Phone Product</td>
<td>Default value: Cisco 9971</td>
</tr>
<tr>
<td>Default CUCM Phone Protocol</td>
<td>Default value: SIP</td>
</tr>
<tr>
<td>Default CUCM Phone Softkey Template</td>
<td>Default value: Standard User</td>
</tr>
<tr>
<td>Default CUCM Phone SIP Profile</td>
<td>Default value: Standard SIP Profile</td>
</tr>
</tbody>
</table>
From the **Line Defaults** tab, click the following fields to modify their default values as required. These default values are applied to the configuration template associated with adding a line (line-cft).

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default CUCM Line Call Forward On Failure</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Internal CSS</td>
<td></td>
</tr>
<tr>
<td>Default CUCM Line Call Forward Busy</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Internal CSS</td>
<td></td>
</tr>
<tr>
<td>Default CUCM Line Call Forward Not</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Registered CSS</td>
<td></td>
</tr>
<tr>
<td>Default CUCM Line Call Forward No Coverage</td>
<td>Default value: None</td>
</tr>
<tr>
<td>CSS</td>
<td></td>
</tr>
</tbody>
</table>

---

**Step 6**

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default CUCM Phone Security Profile</td>
<td>Default value: Cisco 9971 - Standard SIP Non-Secure Profile</td>
</tr>
<tr>
<td>Default CUCM Phone Presence Group</td>
<td>Default value: Standard Presence group</td>
</tr>
<tr>
<td>Default CUCM Phone Enable Extension Mobility</td>
<td>Default value: Off</td>
</tr>
<tr>
<td>Default CUCM Phone Common Device Config</td>
<td>Default value: Standard Common Phone Profile</td>
</tr>
<tr>
<td>Default CUCM Remote Destination DND Option</td>
<td>Default value: Call Reject</td>
</tr>
<tr>
<td>Default CUCM Device Profile Line E164 Mask</td>
<td>Default value: Site Dial Plan Published Number</td>
</tr>
<tr>
<td>Default CUCM SIP Profile</td>
<td>Default value: Standard SIP Profile</td>
</tr>
<tr>
<td>Default CUCM Phone Subscribe CSS</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Default CUCM Remote Destination Profile CSS</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Default CUCM User Subscribe CSS</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Default CUCM Phone Line E164 Mask</td>
<td>Default value: Site Dial Plan Published Number</td>
</tr>
<tr>
<td>Default CUCM Remote Destination Profile ReRouting CSS</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Default CUCM Remote Destination Profile Line E164 Mask</td>
<td>Default value: Site Dial Plan Published Number</td>
</tr>
<tr>
<td>Default CUCM Device CSS</td>
<td>Default value: Cu{CustomerId}Si{SiteId}-{countryIsoCode}-DP-Emer-CSS</td>
</tr>
<tr>
<td>Default CUCM Device Profile EMCC CSS</td>
<td>Default value: None</td>
</tr>
</tbody>
</table>
### Step 7
From the **User Defaults** tab, click the following fields to modify their default values as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default System User Role</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Default CUCM User Presence Group</td>
<td>Default value: Standard Presence group</td>
</tr>
<tr>
<td>Default CUCM User PIN</td>
<td>Default value: 12345</td>
</tr>
<tr>
<td>Default CUCM User Password</td>
<td>Default value: cisco123</td>
</tr>
</tbody>
</table>

### Step 8
From the **CUC Defaults** tab, click the following fields to modify their default values as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default CUC SMPP Provider</td>
<td>Default value: None</td>
</tr>
</tbody>
</table>
Option | Default Value
--- | ---
Default CUC Phone System | This field is populated by the Voice Mail workflow when a Voice Mail pilot number is associated with a site. Likewise, the field is reset (Empty) when the Voice Mail pilot number is disassociated from a site.
Default CUC Subscriber Template | This field is populated by the Voice Mail workflow when a Voice Mail pilot number is associated with a site. Likewise, the field is reset (Empty) when the Voice Mail pilot number is disassociated from a site.
Default CUC HTML Notification Template | Default value: Default_Dynamic_Icons

Step 9 From the HotDial Defaults tab, click the following fields to modify their default values as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default PLAR CSS</td>
<td>Default value: None</td>
</tr>
<tr>
<td>Default HotDial Time Zone</td>
<td>Default value: None</td>
</tr>
</tbody>
</table>

Step 10 Click Save to save the modified site defaults.

---

**Cisco Hosted Collaboration Solution Roles and Privileges**

Depending on the role assigned, an administrator has the following Dial Plan privileges:

**Note**

Administrators can perform all tasks associated with their roles, as well as all Dial Plan tasks that are lower on the navigation hierarchy. Hierarchy is shown from left (highest) to right (lowest) in the table below.

**Table 1: Cisco HCS Dial Plan Roles and Privileges**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>HCS Admin</th>
<th>Provider / Reseller Admin</th>
<th>Customer Admin</th>
<th>Site Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Customer Dial Plan</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td></td>
</tr>
<tr>
<td>Create a Site Dial Plan</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td></td>
</tr>
<tr>
<td>Configure Class of Service</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td></td>
</tr>
<tr>
<td>Configure Short Code</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X</td>
</tr>
<tr>
<td>Tasks</td>
<td>HCS Admin</td>
<td>Provider / Reseller Admin</td>
<td>Customer Admin</td>
<td>Site Admin</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------</td>
<td>----------------------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Configure Directory Number Routing</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X</td>
</tr>
<tr>
<td>Add Site Directory Numbers</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X</td>
</tr>
<tr>
<td>View Directory Number Inventory</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X</td>
</tr>
<tr>
<td>Configure SIP Route Patterns</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X</td>
</tr>
<tr>
<td>Create Voice Mail Service</td>
<td>X (Provider/Reseller level)</td>
<td>X (Provider/Reseller level)</td>
<td>X (Provider/Reseller level)</td>
<td>X</td>
</tr>
<tr>
<td>Associate Voice Mail Services to Customer</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X</td>
</tr>
<tr>
<td>Define a Voice Mail Pilot Number</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X</td>
</tr>
<tr>
<td>Associate Pilot Numbers to a Site</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X</td>
</tr>
<tr>
<td>Configure SIP Trunks</td>
<td>X (Provider/Reseller level)</td>
<td>X (Provider/Reseller level)</td>
<td>X (Provider/Reseller level)</td>
<td>X</td>
</tr>
<tr>
<td>Reset SIP Trunks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Restart SIP Trunks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Configure Route Groups</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Configure Route Lists</td>
<td>X (Customer or Site level)</td>
<td>X (Customer or Site level)</td>
<td>X (Customer or Site level)</td>
<td>X</td>
</tr>
<tr>
<td>Associate Local Route Groups to a Device Pool</td>
<td>X (Customer or Site level)</td>
<td>X (Customer or Site level)</td>
<td>X (Customer or Site level)</td>
<td>X</td>
</tr>
<tr>
<td>Provision Emergency Calls</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Create Schemas</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Modify Site Defaults</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X (Site level)</td>
<td>X</td>
</tr>
<tr>
<td>Assign Custom Schemas to Customers</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X (Customer level)</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note**

For more information on bulk loading and Cisco HCS Intelligent Loader, see *Cisco Unified Communications Domain Manager, Release 10.6(1) Bulk Loader Provisioning Guide.*
## Northbound Notification

The Cisco Unified Communications Domain Manager 10.6(1) Northbound Notification (NBN) provides a mechanism to notify an Operations Support System (OSS) or Business Support System (BSS) when user data in Cisco Unified Communications Domain Manager 10.6(1) is created, updated, or deleted. The Northbound Notifications can be customized to specify which events trigger notification and the destination of notifications.

The supported model types are:

**data/NormalizedUser**

Essential user information. Changes occur either from LDAP synch or manually in Cisco Unified Communications Domain Manager 10.6(1).

**relation/Subscriber**

Subscriber information, such as assigned devices and services. Only changes made in Cisco Unified Communications Domain Manager 10.6(1) via Subscriber Management generate notifications. Changes to subscribers made in Cisco Unified Communications Manager do not generate notifications.

All NBN events are post-execution so the notification is sent immediately after the data is changed in Cisco Unified Communications Domain Manager 10.6(1).
Notification Format

Failing changes to user data result in a pair of notifications, one for the attempted change and an opposite one for the rollback of the change. For example, a failing user add generates a create notification and a delete notification.

To suspend notifications for a given model type and operation, mark the event as 'inactive' and notifications will neither be sent nor stored while the event is inactive. Once the event is marked as 'active', subsequent notifications will be sent.

The Northbound Notifications are sent to a destination as HTTP or HTTPS POST requests. The message body is a JSON map that contains the notification data. The JSON map is in the following format:

<table>
<thead>
<tr>
<th>Key</th>
<th>Datatype</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>model_type</td>
<td>String</td>
<td>All</td>
</tr>
<tr>
<td>operation</td>
<td>String</td>
<td>All</td>
</tr>
<tr>
<td>pkid</td>
<td>String</td>
<td>All</td>
</tr>
<tr>
<td>hierarchy</td>
<td>String</td>
<td>All</td>
</tr>
<tr>
<td>new_data</td>
<td>Map</td>
<td>Create/Update</td>
</tr>
<tr>
<td>previous_data</td>
<td>Map</td>
<td>Update/Delete</td>
</tr>
</tbody>
</table>

The keys in the new_data and old_data maps are the attribute names for the given model type.

Example

See the following example of a notification's message body triggered by updating a user:

```json
{
    'model_type': 'data/NormalizedUser',
    'operation': 'update',
    'pkid': '5445310900698a11d83164e3',
    'hierarchy': '543c57ea00698a11d8305815',
    'new_data': {
        'username': 'jdoe',
        'mail': ['jdoe@provider.com'],
        'givenName': ['Jane'],
        'sn': ['Doe'],
        'l': ['RTP']
    },
    'previous_data': {
        'username': 'jdoe',
        'mail': ['jdoe@provider.com'],
        'givenName': ['Jane'],
        'sn': ['Doe'],
        'l': ['New York']
    }
}
```
NBN Transaction Processing

Once an NBN event is triggered, it is handled in a new transaction independent of the original transaction that triggered the event. These transactions can also be queried through the transaction log. The result of the NBN transaction will be successful if a positive HTTP or HTTPS response code is received from the OSS/BSS. If no response is received (timeout) or a negative response code is received, the transaction will show as failed.

Northbound Notification Workflow

Perform the following procedures to configure northbound notification.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure Northbound Notification Destination, on page 49 to specify the destination for northbound notifications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure Northbound Notification Event, on page 51 to specify an event to trigger the northbound notification.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure Northbound Notification Event Attributes, on page 50 to specify the list of attributes to be received in a notification for a specific event.</td>
</tr>
</tbody>
</table>

*Note* Steps 2 and 3 can be performed in either order, but after the list attributes are defined in Step 3 you will need to edit the event (Step 2) to add or update the Attribute Selector field.

Configure Northbound Notification Destination

Use this procedure to set the destination for Northbound Notifications of Cisco Unified Communications Domain Manager 10.6(1) events. Only one NBN destination can be configured.

*Note* You cannot delete a destination until it is removed or disassociated from all events.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Login as the provider admin.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Administration Tools &gt; Northbound Notifications &gt; Destination.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Provide the following information for the destination:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/IP Address</td>
<td>Hostname or IP address of the OSS/BSS http server. This field is mandatory.</td>
</tr>
<tr>
<td>Port</td>
<td>The destination port. This field is mandatory.</td>
</tr>
</tbody>
</table>
### Configure Northbound Notification Event Attributes

You can use attribute selectors to define the attributes to be received in a notification for a particular event. Notifications contain only the specified fields and are not sent if none of the fields are chosen.

**Note**
You cannot delete an attribute selector until it is removed or disassociated from all events.

**Important**
It is possible to create an attribute selector through the API with “invalid” attributes as there is no API validation on the list of attributes. We recommend using the GUI or API to retrieve the list of attributes prior to creating an attribute list through the API. Refer to *Cisco Unified Communications Domain Manager, Release 10.6(1) API Reference Guide*. If an invalid attribute is added to an attribute filter, the transaction will succeed but notifications will not contain the chosen field.

### Procedure

**Step 1** Login as the provider admin.

**Step 2** Select **Administration Tools > Northbound Notifications > Attributes**.

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

**Step 4** Enter a unique name.

**Step 5** Select a model type: either data/NormalizedUser or relation/Subscriber.

**Step 6** Highlight one or more attributes and perform the following:

- Click **Select** to add an attribute to the list of chosen attributes. You can also select multiple attributes at a time by highlighting them and clicking **Select**. The attributes move from the Available box to the Selected box.

- Click **Remove** to remove an attribute from the list of chosen attributes. You can also remove multiple attributes at a time by highlighting them and clicking **Remove**. The attributes from the Selected box to the Available box.
Example:
For the data/NormalizedUser model, you could select Username, First Name, Last Name, Phone Number, and Mail. Notifications are then sent when an event occurs that includes one or more of these attributes.

Step 7
Click Save.

What to Do Next
Apply the event attributes to an event by adding or updating the event and choosing the desired attribute selector.

Configure Northbound Notification Event

Use this procedure to specify an event to trigger Northbound Notifications.

Before You Begin
You must set the Northbound Notification Destination before you can configure events.

Procedure

Step 1
Login as the provider admin.

Step 2
Select Administration Tools > Northbound Notifications > Events.

Step 3
Click Add.

Step 4
Provide the following information for the triggering event:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Event name. Must be unique. This field is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the event</td>
</tr>
<tr>
<td>Active</td>
<td>Check to turn on notification.</td>
</tr>
<tr>
<td>Model Type</td>
<td>Select either data/NormalizedUser or relation/Subscriber as the model type of the data that triggers the event. This field is mandatory.</td>
</tr>
<tr>
<td>Operation</td>
<td>Select from the operations applicable to the selected model type. This field is mandatory.</td>
</tr>
<tr>
<td>Attribute Selector</td>
<td>Set an attribute selector to restrict (filter) the list of attributes sent in notifications for this event. This field is optional. To remove an existing attribute selector, backspace and delete it from the Attribute Selector field. If you do not specify an attribute selector, all possible attributes are sent in notifications for this event.</td>
</tr>
</tbody>
</table>
### Configure Northbound Notification Event

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The provider's NBN destination. This field is read only.</td>
</tr>
</tbody>
</table>

**Step 5** Click Save.
CHAPTER 7

LDAP Management

- Enable LDAP Integration, page 53
- Set Up LDAP User Sync, page 54
- Sync Users from LDAP, page 55

Enable LDAP Integration

Follow these steps to enable LDAP integration with Active Directory (AD) or OpenLDAP. Note the following limitations:

- Only one LDAP server can be enabled at each hierarchy node. Attempting to enable more than one causes the transaction to fail.
- Adding the same LDAP server with the same Search Base DN to any of the related hierarchies causes the LDAP server addition transaction to fail.

Procedure

**Step 1**
Log in at any hierarchy node.

**Step 2**
Set the hierarchy node to the desired node where you want the users synchronized.

**Step 3**
Navigate to **LDAP Management > LDAP Server**.

**Step 4**
Click **Add**.

**Step 5**
Complete the fields:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Defaults to the current hierarchy level</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of the LDAP server. This field is required.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number for LDAP traffic. Defaults to 389.</td>
</tr>
<tr>
<td>User DN</td>
<td>The User Distinguished Name on the LDAP server. This field is required.</td>
</tr>
</tbody>
</table>
Set Up LDAP User Sync

Set Up LDAP User Sync

Follow these steps to add an LDAP User Sync object. This is the object that syncs users from the configured LDAP directory into Cisco Unified Communications Domain Manager 10.6(1). The users then appear at the hierarchy node at which the LDAP User Sync object exists and can be managed through User Management menu options (for example, move users to other hierarchies, push to Cisco Unified Communications Manager).

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Navigate to <strong>LDAP Management &gt; LDAP User Sync</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>
| **Step 3** | Select the User Model Type.  
If the LDAP server is Active Directory, the default is device/ldap/user.  
If the LDAP server is OpenLDAP, the default is device/ldap/inetOrgPerson. |
To identify a non-default User Model Type to use from the LDAP schema, contact the LDAP administrator responsible for the LDAP server from which you are synching users.

**Step 4**
Select the User Role to be assigned to all synchronized users. This value can be changed manually for individual users after synchronization.

**Step 5**
Select move, delete, and purge modes.

- **User Move Mode**—indicates whether users are automatically moved based on the filters defined ([User Management > Define Filters](#)).
- **User Delete Mode**—indicates whether users are automatically deleted from Cisco Unified Communications Domain Manager 10.6(1) if they are deleted from the LDAP directory. If set to automatic, all subscriber resources associated with the user, such as phone, are also deleted.
- **User Purge Mode**—indicates whether users are automatically deleted from Cisco Unified Communications Domain Manager 10.6(1) if they are purged from the LDAP device model. The purge operation can be initiated by the admin to remove the LDAP user from the device layer even if the user has not been removed from the LDAP directory.

**Step 6**
Click the **Field Mappings** tab and enter the following required mappings:

- **LDAP Username** (for example, sAMAccountName)
- **Surname**
- **EmailAddress**

**Step 7**
(Optional) Complete other field mappings as desired, for other operations such as pushing users to Cisco Unified Communications Manager or creating move filters.

**Step 8**
Click **Save**.

An LDAP sync is scheduled, but not activated by default. See [Sync Users from LDAP](#), on page 55.

---

**Sync Users from LDAP**

Users can be synced from LDAP by activating a scheduled sync, or by doing an manual sync.

---

**Note**
A sync cannot be cancelled and an LDAP server cannot be deleted while a sync is in progress.

### Procedure

**Step 1**
To activate a scheduled LDAP sync:

a) Navigate to **LDAP Management > LDAP Schedule**.
b) Click an LDAP Schedule.
c) Check the **Active** checkbox.
d) Click Save.

Step 2  To manually perform an LDAP sync:
   a) Set the hierarchy to the location of the LDAP server.
   b) Navigate to User Management > Sync & Purge Users
   c) In the Action menu, select Synchronize users from LDAP.
   d) Click Save.

Cisco Unified Communications Domain Manager 10.6(1) attempts to sync users from the LDAP server. It may take a few minutes for the users to show up in Cisco Unified Communications Domain Manager 10.6(1).

What to Do Next
Navigate to User Management > Users and verify that users have been synchronized from LDAP.
User Management

- User Management Overview, page 58
- Create User, page 58
- Manage Local Administrators and Operators, page 59
- Define a Filter, page 60
- Methods to Push Users to Cisco Unified Communications Manager, page 61
- Automatic User Push to Cisco Unified Communications Manager, page 61
- Manual User Push to Cisco Unified Communications Manager, page 62
- Automatic Cisco Unified Communications Manager User Move, page 63
- Move Users, page 64
- Check User Provisioning Status, page 65
- Sync and Purge LDAP Users, page 65
- Sync Cisco Unified Communications Manager Users, Lines, and Phones, page 66
- Manage Duplicate User Names, page 67
- Assign a Credential Policy to a User, page 68
- Assign a Credential Policy to an Administrator, page 69
- Unlock a Locked Out User, page 69
- Unlock a Locked Out Administrator, page 69
- Manually Disable User Account, page 70
- Manually Disable Administrator Account, page 70
- Password Management, page 71
- Self Service, page 75
User Management Overview

Users are added to Cisco Unified Communications Domain Manager 10.6(1) from the following potential sources:

- Synched in from LDAP
- Synched from Cisco Unified Communications Manager
- Bulk loader template
- Manually created

Typically users are associated with a Site. You can create move filters to automatically assign users to Sites when they are synched from LDAP or Cisco Unified Communications Manager.Bulk loaded and manually created users can be moved using filters or by individually selecting users.

If an IdP server is deployed at a given hierarchy node above Site, then Cisco Unified Communications Domain Manager 10.6(1) can be configured to provide Single Sign On support for users created or synched in at that hierarchy node.

Conflicts between users synched from different sources are handled according to the strategy described in Manage Duplicate User Names, on page 67. For information about user password management, depending on the source of the user, see Password Management, on page 71.

Users associated with a site can be pushed to the Cisco Unified Communications Manager that appears in the Network Device List assigned to that site. Once pushed to Cisco Unified Communications Manager, users become subscribers that can be provisioned with various collaboration services.

When a user is added to Cisco Unified Communications Domain Manager 10.6(1) by any of the above methods, if the user's language is not set, the user's language is inherited from nearest hierarchy node (at or above the user's node) that has a default language set. If no default language is set anywhere in the hierarchy at or above the user's node, the user's language is set to English.

Create User

To manually create a user do the following:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in as the admin at the hierarchy node where you want to create the user.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select User Management &gt; Users.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 4</td>
<td>At a minimum, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Login username. This field is mandatory.</td>
</tr>
<tr>
<td>Role</td>
<td>Select the user's role. This field is mandatory.</td>
</tr>
</tbody>
</table>
A user is created. If SSO is enabled for the hierarchy node where the user is added, the corresponding SSO user is created.

**Note**  
Because IdPs are not configured at the site hierarchy node, SSO can be enabled for a user created at the site level only by selecting Single Sign On > SSO User, clicking Add, and choosing the appropriate IdP that can authenticate the user.

### Manage Local Administrators and Operators

Default local Cisco Unified Communications Domain Manager 10.6(1) administrators are created when provider, reseller, customer, and site hierarchy nodes are established. Use this procedure to modify or create additional local administrators or operators. Also use this procedure to create administrators for intermediate nodes.

An administrator for a particular hierarchy level can create or modify the administrators and operators at that hierarchy level and any level below. For example, a Customer XYZ administrator can create other Customer XYZ administrators as well as site administrators for Customer XYZ.

**Procedure**

**Step 1**  
Log in as an administrator.

**Step 2**  
To create or modify an admin or operator at a level below your current level, set the hierarchy path at the top of the window.  
For example, if you have logged in as provider admin, and want to create a customer admin, set the hierarchy path to the customer for which you want to create the admin.

**Step 3**  
Select User Management > Local Admins.

**Step 4**  
At a minimum, complete the following fields:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Login username. This field is mandatory.</td>
</tr>
<tr>
<td>Email Address</td>
<td>User email address. This field is mandatory.</td>
</tr>
<tr>
<td>Password</td>
<td>Set the password. This field is mandatory.</td>
</tr>
</tbody>
</table>

**Step 5**  
To modify an existing administrator or operator, click the administrator or operator.
a) Modify the appropriate settings for the admin or operator.
b) Click Save.

## Define a Filter

You can define a Filter to easily select multiple users to move according to one or more user attributes.

If you specify multiple attributes, a user will match the filter only if the user matches all of the attributes in the filter. For example, a filter with State=Missouri and City=Kansas City, would not match a user in Kansas City, Kansas.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select User Management &gt; Define Filters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Provide the following information:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the filter. This field is mandatory.</td>
</tr>
<tr>
<td>Move To Hierarchy</td>
<td>Select the target hierarchy node. This field is mandatory.</td>
</tr>
<tr>
<td>Move To Role</td>
<td>Select the role to be assigned to the user after the move. The available roles depend on the target hierarchy node selected. This field is mandatory.</td>
</tr>
<tr>
<td>Condition</td>
<td>Select a condition for a filter. This field should be set for at least one of the available filters.</td>
</tr>
<tr>
<td>Value</td>
<td>Specify the value to evaluate for the condition. This field should be set for at least one of the available filters.</td>
</tr>
</tbody>
</table>

**Example:**

Set the City Filter to Condition = isexactly and Value = Toronto to move users located in Toronto to the target hierarchy node and give them the target user role.

| Step 4 | Click Save. |

The Filter is available to be used to manually move users by selecting User Management > Move Users. Filters are automatically applied during LDAP and Cisco Unified Communications Manager user synchronization, if the User Move mode is set to automatic.
Methods to Push Users to Cisco Unified Communications Manager

When you manage users in Cisco Unified Communications Domain Manager 10.6(1) there are several steps required to process the new users introduced into the system from the three sources: a synchronization from LDAP directory, a synchronization from Cisco Unified Communications Manager, and a manual configuration in Cisco Unified Communications Domain Manager 10.6(1).

One of these steps is to push the user to the Cisco Unified Communications Manager assigned to the customer and site where the user was added. You can push the user to Cisco Unified Communications Manager from Cisco Unified Communications Domain Manager 10.6(1) in two ways:

1 Automatic Push—Enabled or disabled using the Auto Push to CUCM checkbox from Site Management > Sites
2 Manual Push—Performed from User Management > Manage Users

There are a variety of options available in Cisco Unified Communications Domain Manager 10.6(1) for configuring users with phones, lines, and features. Depending on the option you choose, you may, or may not, want to automatically push users to Cisco Unified Communications Manager.

To determine if you should automatically push users to Cisco Unified Communications Manager, consider the following guidelines:

- When users are synchronized into Cisco Unified Communications Domain Manager 10.6(1) from an LDAP server, or the users are configured locally on Cisco Unified Communications Domain Manager 10.6(1), and then the Subscriber Management > Subscribers menu is used to provision phones, lines, and features for those users, we recommend an automatic user push to Cisco Unified Communications Manager. It does not matter whether you perform the Subscribers configuration through the GUI, bulk loaders, or API; we recommend automatic user push to Cisco Unified Communications Manager in all cases.
- When users are configured locally on Cisco Unified Communications Manager and synchronized into Cisco Unified Communications Domain Manager 10.6(1), the users are already on Cisco Unified Communications Manager, so automatic push to Cisco Unified Communications Manager is not required.

Automatic User Push to Cisco Unified Communications Manager

You can enable Automatic User Push to Cisco Unified Communications Manager by checking the Auto Push Users to CUCM box on the Site Management > Sites > Site Details page. Automatic User Push is disabled by default.

Users are automatically pushed to a Cisco Unified Communications Manager in the following situations:

- When users are moved to a site hierarchy level (either by filters, username, or usernames):
  - If a Network Device List (NDL) is configured on that site and contains a Cisco Unified Communications Manager, the users are pushed to the Cisco Unified Communications Manager.
  - If an NDL is configured on that site with no Cisco Unified Communications Manager, nothing happens.
• If an NDL is not configured on that site, nothing happens.

• When an NDL is added to a site after the site was created:
  • If the NDL is configured with a Cisco Unified Communications Manager, the users at the associated site are pushed.
  • If the NDL is not configured with a Cisco Unified Communications Manager, nothing happens.

• When a Cisco Unified Communications Manager is added to an NDL:
  If the NDL is associated with a site, the users on that site are pushed to the new Cisco Unified Communications Manager.

• When a new user is created at the site level:
  • If an NDL is configured on that site and contains a Cisco Unified Communications Manager, the user is pushed to the Cisco Unified Communications Manager.
  • If an NDL is configured on that site with no Cisco Unified Communications Manager, nothing happens.
  • If an NDL is not configured on that site, nothing happens.

Manual User Push to Cisco Unified Communications Manager

You can manually push users to Cisco Unified Communications Manager from hierarchy nodes between customer and site, inclusive.

--------------------------

Note

The following limitations exist when pushing users to Cisco Unified Communications Manager:

• A user may be pushed to only one Cisco Unified Communications Manager.
• Users with the SelfService role may be pushed only from a site.

--------------------------

Note

For users that have been synched from LDAP, you can use **Subscriber Management > Quick Add Subscriber** to push the users to Cisco Unified Communications Manager, instead of this procedure.
### User Management

**Automatic Cisco Unified Communications Manager User Move**

Use this procedure to automatically move users synced from Cisco Unified Communications Manager using previously-defined move filters.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Navigate to <strong>Device Management &gt; CUCM &gt; Servers</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click the Cisco Unified Communications Manager server to modify.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click the <strong>Publisher</strong> tab.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>From the User Move Mode drop-down list, select <strong>Automatic</strong>.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Subsequently synced Cisco Unified Communications Manager users are automatically moved based on previously-defined user management move filters.
Move Users

Users can be moved between any hierarchy nodes, with the exception of hierarchy nodes above the hierarchy level at which they were originally created or synced in. For example, customer users cannot be moved to a reseller hierarchy node. A common practice might be to move users synced in at a customer hierarchy node to various customer sites.

Note

The following additional limitations exist when moving users that have been pushed to Cisco Unified Communications Manager:

- Cisco Unified Communications Manager users can be moved only down the hierarchy.
- An NDL containing the same Cisco Unified Communications Manager that the users were pushed to must be referenced at or below the target hierarchy node.

You can select the users to be moved in the following three ways:

- Move users by filters—allows you to select the users depending on one or more user attributes, for example City or Street
- Move users by usernames—allows you to select multiple users by their usernames
- Move user by username—allows you to move an individual user

When you move users, you select a Move To Role for the users that is appropriate for the target hierarchy node.

Procedure

Step 1
Log in at the appropriate hierarchy level.

Step 2
Select User Management > Move Users.

Step 3
In the Action field, select the move method.

- If you select Move users by filters:
  1. Select one or more Move Filters from the Available list and click Select to move them to the Selected list. You can select filters in a different order to change the order in which they are applied.
  2. Click Save to move the users that are defined by the move filters.

- If you select Move users by usernames:
  1. Select the target hierarchy node from the Move To Hierarchy menu. The Move To Role field appears.
  2. Select the target user role from the Move To Role menu.
  3. Select the users you want to move or click Select All.
  4. Click Save to move the users.

- If you select Move user by username:
  1. Select the username from the User menu. The Move To Hierarchy field appears.
  2. Select the target hierarchy node from the Move To Hierarchy menu. The Move To Role field appears.
3. Select the target user role from the Move To Role menu.
4. Click Save to move the user.

For information about user roles, see Roles, on page 2.

Step 4 Select User Management > Users to verify that the users are moved to the target hierarchy.

Check User Provisioning Status

Procedure

Step 1
Login as a provider, reseller, or customer admin.

Step 2
Select User Management > Provisioning Status.

Step 3
The following information is displayed for each user that is visible to the admin:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>User’s username</td>
</tr>
<tr>
<td>CUCM Server</td>
<td>Cisco Unified Communications Manager to which the user is synched</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>LDAP from which the user is synched</td>
</tr>
<tr>
<td>Synced To</td>
<td>Hierarchy level where the user was originally synched to or created from</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>User’s current hierarchy node</td>
</tr>
</tbody>
</table>

You can sort the table by clicking on the field headings. You can search any field where a magnifying glass appears when the cursor is on the field heading.

Sync and Purge LDAP Users

Use this procedure to sync or purge Users synced from an LDAP server.

Procedure

Step 1
Set the hierarchy path to the hierarchy node where the LDAP server is.

Step 2
Click User Management > Sync & Purge > LDAP Users.

Step 3
Provide the information as shown below:
### Field | Description
---|---
Remove Log Messages | Select if you want to remove user management logs prior to the action.  
Remove Log Direction | Select Local to remove logs at the hierarchy of the LDAP server. Select Down to remove logs at and below the hierarchy of the LDAP server. This field appears only if Remove Log Messages is checked.  
Action | Select synchronize or purge. This field is mandatory.  

**Step 4**  
Click **Save** to initiate the sync or purge action.

---

### Sync Cisco Unified Communications Manager Users, Lines, and Phones

Use this procedure to sync Users, Lines, and Phones from Cisco Unified Communications Manager.

**Note**  
Syncing of lines and phones is meant only for self-provisioning and is not intended for a full migration scenario. Only Jabber and desk phones are supported for sync from Cisco Unified Communications Manager. Single Number Reach and Extension Mobility are not supported in terms of adding to Cisco Unified Communications Manager first and then syncing into Cisco Unified Communications Domain Manager.

**Procedure**

1. **Step 1**  
   Set the hierarchy path to the hierarchy node where the Cisco Unified Communications Manager server is.
2. **Step 2**  
   Click **User Management > Sync & Purge > CUCM Users, Lines, and Phones**.
3. **Step 3**  
   Provide the information as shown below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Log Messages</td>
<td>Select if you want to remove user management logs prior to the action.</td>
</tr>
<tr>
<td>Remove Log Direction</td>
<td>Select Local to remove logs at the hierarchy of the selected Cisco Unified Communications Manager. Select Down to remove logs at and below the hierarchy of the selected Cisco Unified Communications Manager. This field appears only if Remove Log Messages is checked.</td>
</tr>
<tr>
<td>Action</td>
<td>Select synchronize. This field is mandatory.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Cisco Unified CM | Select the Cisco Unified Communications Manager server. Data will be synced from the selected Cisco Unified Communications Manager. This field is mandatory.

**Step 4** Click **Save** to initiate the sync action.

---

### Manage Duplicate User Names

Users are created in an LDAP sync, a Cisco Unified Communications Manager sync, or manually in the Cisco Unified Communications Domain Manager 10.6(1) GUI. All users are created according to the following duplicate username guidelines:

- The username of a user cannot be updated if another user in the current hierarchy has the same username. This includes **above, below, or at the same level** in the current hierarchy.
- A user cannot be added if another user that is **above, or was originally above before being moved**, in the current hierarchy has the same username.
- A user cannot be manually added if another user that is **at the same level or below** in the current hierarchy has the same username.
- A user may or may not be synched in from LDAP or Cisco Unified Communications Manager if another user that is **at the same level or below** in the current hierarchy has the same username, depending on the source of the existing user as shown in the tables below:

#### Table 2: Users created in an LDAP Sync

<table>
<thead>
<tr>
<th>Original source of existing user</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Simple user update, if the user is coming from the same LDAP server.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Update user + update provisioning status with LDAP server and SyncTo info</td>
</tr>
<tr>
<td>Manually created</td>
<td>Update user + update provisioning status with LDAP server and SyncTo info</td>
</tr>
</tbody>
</table>

#### Table 3: Users created in a Cisco Unified Communications Manager Sync

<table>
<thead>
<tr>
<th>Original source of existing user</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>User is not synced.</td>
</tr>
<tr>
<td>Original source of existing user</td>
<td>Action</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Simple user update, if the user is coming from the same Cisco Unified Communications Manager server.</td>
</tr>
<tr>
<td>Manually created</td>
<td>Update user + update provisioning status with Cisco Unified Communications Manager server and SyncTo info</td>
</tr>
</tbody>
</table>

**Note**

If a user cannot be created or updated during an LDAP or Cisco Unified Communications Manager sync, a log is created in **User Management > Log Messages** and the sync completes successfully. If a user cannot be created or updated manually, an error message is generated.

**Important**

An update is blocked if two duplicate users are from the same source but originate from different servers.

---

### Assign a Credential Policy to a User

In general, a user will inherit a credential policy from the nearest hierarchy node at or above the user's location that has a default credential policy set. However, you can explicitly assign a credential policy to a user.

**Procedure**

1. **Step 1** Log in as provider, reseller, or customer admin.
2. **Step 2** Select **User Management > Users**.
3. **Step 3** Click the user that you want to assign a credential policy to.
4. **Step 4** Click the **Account Information** tab.
5. **Step 5** In the Credential Policy field, select the credential policy from the pulldown menu. The menu contains all the credential policies available at or above the user's node in the hierarchy.
6. **Step 6** Click **Save**.

**Note**

If a user is already logged in when the credential policy is changed, changes do not take effect until the user logs out and logs in again.
Assign a Credential Policy to an Administrator

In general, an administrator will inherit a credential policy from the nearest hierarchy node at or above the administrator's location that has a default credential policy set. However, you can explicitly assign a credential policy to an administrator.

**Procedure**

| Step 1 | Log in as provider, reseller, or customer administrator. |
| Step 2 | Select User Management > Local Admins. |
| Step 3 | Click the administrator that you want to assign a credential policy to. |
| Step 4 | Click the Account Information tab. |
| Step 5 | In the Credential Policy field, select the credential policy from the pulldown menu. The menu contains all the credential policies available at or above the administrator's node in the hierarchy. |
| Step 6 | Click Save. |

**Note** If an administrator already logged on when the credential policy is changed, changes do not take effect until the administrator logs out and logs on again.

Unlock a Locked Out User

If a user is locked out on account of a credential policy violation, an administrator responsible for the user can unlock the user's account.

**Procedure**

| Step 1 | Login as provider, reseller, or customer admin. |
| Step 2 | Select User Management > Users. |
| Step 3 | Click the user whose account you want to unlock. |
| Step 4 | Click the Account Information tab. |
| Step 5 | Uncheck the Locked check box. |
| Step 6 | Click Save. |

Unlock a Locked Out Administrator

If an administrator is locked out on account of a credential policy violation, an administrator at a hierarchy node above the locked out administrator can unlock the administrator's account.
Procedure

Step 1: Login as provider, reseller, or customer admin, depending on the location of the locked out administrator.
Step 2: Select User Management > Local Admins.
Step 3: Click the administrator whose account you want to unlock.
Step 4: Click the Account Information tab.
Step 5: Uncheck the Locked check box.
Step 6: Click Save.

Manually Disable User Account

Usually, a user account is disabled when the password has expired. However, an administrator can manually disable a user account at any time.

Note
Manually disabling a user is preferred to manually locking out a user as you can provide the reason for disabling.

Procedure

Step 1: Log in as provider, reseller, or customer admin.
Step 2: Select User Management > Users.
Step 3: Click the user whose account you want to disable.
Step 4: Click the Account Information tab.
Step 5: Check the Disabled check box.
Step 6: Enter the reason the account is disabled in the Reason for Disabled field. This reason will be displayed to the user when the next login attempt fails.
Step 7: Click Save.

Manually Disable Administrator Account

Usually, an administrator account is disabled when the password has expired. However, an administrator at a higher hierarchy level can manually disable an administrator account at any time.

Note
Manually disabling an administrator is preferred to manually locking out an administrator as you can provide the reason for disabling.
Procedure

| Step 1 | Log in as provider, reseller, or customer admin. |
| Step 2 | Select User Management > Local Admins. |
| Step 3 | Click the administrator whose account you want to disable. |
| Step 4 | Click the Account Information tab. |
| Step 5 | Check the Disabled check box. |
| Step 6 | Enter the reason the account is disabled in the Reason for Disabled field. This reason will be displayed to the administrator when the next login attempt fails. |
| Step 7 | Click Save. |

Password Management

The following sections describe the various ways passwords are set by default and can be configured between LDAP, Cisco Unified Communications Domain Manager 10.6(1), and Cisco Unified Communications Manager.

User Synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1)

LDAP Authentication can be enabled on Cisco Unified Communications Domain Manager 10.6(1) and if enabled, when the user is synced, the LDAP password is used to log in. If the user is synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1), the password is not synced with other user information that is pulled from LDAP. However, the password can be used to log in and the local password is ignored for users synced in from LDAP.

User Synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1) (SSO Enabled)

If the user is synced from LDAP to Cisco Unified Communications Domain Manager 10.6(1) with SSO enabled, the passwords are defined and enforced at the IdP.

User Synced from LDAP to Cisco Unified Communications Manager

When a user is synced from LDAP to Cisco Unified Communications Manager, the password is not synced like other user information that is pulled from LDAP. If LDAP Authentication is enabled, the password in the LDAP Server is used unless the password was changed locally in Cisco Unified Communications Manager, forcing the Cisco Unified Communications Manager password to be used. However, if LDAP Authentication is not enabled, the default password is whatever was configured in Cisco Unified Communications Manager as the Default. If there is no default password defined, then one needs to be configured manually.
User Synced from Cisco Unified Communications Domain Manager 10.6(1)

When users are synced from Cisco Unified Communications Manager to Cisco Unified Communications Domain Manager 10.6(1), the password is not transferred over. The passwords are blank and need to be configured by an admin before the accounts can be used.

This applies to Cisco Unified Communications Manager users that were originally added manually to Cisco Unified Communications Manager or synced from LDAP.

User Added Manually from User Management

When a user is added manually through User Management, the password is set to the local Cisco Unified Communications Domain Manager 10.6(1) password that was specified when the user was created. When this type of user is pushed to Cisco Unified Communications Manager, the password is not pushed. Instead the password can be configured in one of the following ways:

Create a Default Password with Cisco Unified Communications Manager

1. Log in to Cisco Unified Communications Manager as an admin.
3. Select the line item that has the Credential User to 'End User' and Credential Type to 'Password'.
4. Enter the default password in the confirmation box and click Save.

Ensure the user has the correct role defined.

Or

Manually Set the Password in the CUCM End User Page

1. Log in to Cisco Unified Communications Manager as an admin.
3. Filter for the user you wish to modify.
4. Change password fields for the specified user.

Force User Password Change

You can use a credential policy to force users to change their passwords on initial login. However, an administrator can manually force a user password change on the next login attempt.
**Procedure**

**Step 1** Log in as provider, reseller, or customer admin.

**Step 2** Select **User Management** > **Users**.

**Step 3** Click the user whose password you want to be changed on the next login attempt.

**Step 4** Click the **Account Information** tab.

**Step 5** Check the **Change Password on Next Login** check box.

**Step 6** Click **Save**.

When the user next attempts to login, the user will be prompted to change the password. Once the password is changed the **Change Password on Next Login** check box is cleared.

---

**Force Administrator Password Change**

You can use a credential policy to force administrators to change their passwords on initial login. However, an administrator at a higher hierarchy level can manually force an administrator to change password on the next login attempt.

**Procedure**

**Step 1** Log in as provider, reseller, or customer admin.

**Step 2** Select **User Management** > **Local Admins**.

**Step 3** Click the administrator whose password you want to be changed on the next login attempt.

**Step 4** Click the **Account Information** tab.

**Step 5** Check the **Change Password on Next Login** check box.

**Step 6** Click **Save**.

When the administrator next attempts to login, the administrator will be prompted to change the password. Once the password is changed the **Change Password on Next Login** check box is cleared.

---

**Manage Your Own Account Password**

Logged in users or administrators can manage their own account passwords.

**Note**

Users who are configured for Single Sign On or through LDAP do not manage their account passwords in Cisco Unified Communications Domain Manager 10.6(1).

**Change Password**

To change your own password when you are logged in to Cisco Unified Communications Domain Manager 10.6(1).
Reset My Password
   To reset your password from the Login page when you have forgotten your password.

Password Reset Questions
   To configure your own password reset questions.

Change Your Own Password
   Follow this procedure to change your own password if required:
   1. Log in to Cisco Unified Communications Domain Manager 10.6(1).
   2. Click the arrow next to the logged in user at the top right-hand side of the screen.
   3. Choose the Change Password option from the drop-down menu. The Change Password screen is displayed.
   4. Enter your existing password in the Old Password field.
   5. Enter your new password in the New Password field.
   6. Confirm your new password by re-entering it in the Repeat New Password field.
   7. Click Change Password in the button bar. Your password is changed.

Reset Your Own Password
   You can reset your password only if you have already provided answers to the security questions created by your administrator.
   If you forget your password while attempting to log in to Cisco Unified Communications Domain Manager 10.6(1):
   1. Enter your username in the Username field on the Log in screen.
   2. Click the Forgot Password? hyperlink located below the Log in button.
   3. Enter your username again.
   4. Click Reset my password.
   5. Click in each security question field and type the correct answer.
   6. Click in the New Password field and type your new password.
   7. Click in the Repeat Password field and re-type your new password.
   8. Click Reset my Password. Your password is changed.
   9. Click the Login hyperlink if you want to attempt to log in again.
Configure Your Own Password Reset Questions

- **Note**: Configuring your own password reset questions is available only if the credential policy applied to your user account has **Number of Questions Asked During Password Reset** set to > 0.

1. Log in to Cisco Unified Communications Domain Manager 10.6(1).
2. Click the arrow next to the logged in user at the top right-hand side of the screen.
3. Choose the **Password Reset Questions** option from the drop-down menu. The Password Reset Questions screen is displayed.
4. Type your password in the **Current Password** field.
5. Choose the required security question from the **Question** drop-down list.
6. Enter your answer to the above question in the **Answer** field.
7. Repeat steps 5 and 6 until you have configured the required amount of security questions (as determined by your administrator).
8. Click the **Update Security Questions** button in the button bar when complete. Your security questions and answers are updated.

Self Service

Using the Cisco Unified Communications Domain Manager 10.6(1) Self Service interface, end users can configure their own phone settings, including voicemail, call forwarding, availability, and speed dials. For detailed information about the Self Service interface, see *Cisco Unified Communications Domain Manager, Release 10.6(1) Self Service Guide*.

To access the Self Service interface, a user must be assigned a SelfService role in Cisco Unified Communications Domain Manager 10.6(1). A user may get a SelfService role in one of the following ways:

- Automatically when synced from LDAP, if the LDAP Sync has User Role configured to a SelfService role.
- By default when synced from Cisco Unified Communications Manager.
- Manually assigned by an administrator using **User Management** > **Users**.

To access the Self Service interface, the user should enter https://<service-ip-or-node-name>/selfservice/#/login?theme=cisco_selfservice in the browser URL field.

- **Note**: Access to the Self Service interface and the Cisco Unified Communications Domain Manager 10.6(1) administrative GUI are mutually exclusive. Therefore, if an administrator needs access to the Self Service interface, the administrator will need a second user configured in Cisco Unified Communications Domain Manager 10.6(1) with a SelfService role assigned to it.
Self Service and End User Configuration

As an Administrator, you can:

• Configure various aspects of the Self Service interface
• Provide end user access to Self Service
• Configure services for the end users as required

The following table provides a summary of the configurable items in Self Service.

Table 4: Configurable Items in Self Service Interface

<table>
<thead>
<tr>
<th>Task or Item</th>
<th>Description</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>End user access</td>
<td>An end user can log into the Self Service GUI if a 'System User' entry exists for the user. A 'System User' entry is created automatically when a user is added as a subscriber.</td>
<td>See Subscriber Management, on page 173</td>
</tr>
<tr>
<td>End user access</td>
<td>You can grant an end user access to Self Service by creating a user, with a Self Service role, directly in the System user interface. Note that such a user will not be able to view devices or any services associated with the devices, nor will a manually-added user be able to view personal information such as first name, last name, address, department, and so on.</td>
<td>See Create User, on page 58</td>
</tr>
<tr>
<td>User Authentication</td>
<td>Self Service authentication is controlled by the administration interface using the same three authentication methods: Standard, LDAP, and SSO.</td>
<td>See &quot;System User&quot; in the User Authentication Management chapter of Cisco Unified Communications Domain Manager, Release 10.6(1) Planning and Install Guide</td>
</tr>
<tr>
<td>GUI Themes and Branding</td>
<td>The Self Service GUI interface can be branded by configuring Cascading Style Sheets and images and logos. It uses the same theme upload and download interface used for the Admin GUI. The theme itself however, is different between the Admin and Self Service interface (based on the user role). The login page theme is also loaded from the URL: https://&lt;host&gt;/selfservice/#/login?theme=mytheme</td>
<td>See Download, Edit and Update a Theme, on page 236</td>
</tr>
<tr>
<td>Task or Item</td>
<td>Description</td>
<td>For More Information</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Personal Phones (Remote Destinations)</td>
<td>You must allocate a remote destination profile (RDP) to an end user for them to be able to manage their own personal phones and simultaneous ring settings. If no RDP is associated to the end user, the Personal Phones management interface in self service is hidden. Note that multiple RDP’s per end user is not supported. The Personal Phones management interface in Self Service is also hidden if an end user has more than one RDP associated.</td>
<td>See Cisco Unified Communications Domain Manager, Release 10.6(1) Self Service Guide</td>
</tr>
<tr>
<td>Dual Mode Phones - Mobile ID</td>
<td>If a user has a dual mode device associated, they can manage the phone number and simultaneous ring settings for the device. If no dual mode device is associated, the relevant settings are hidden in the Self Service interface.</td>
<td>See Configure Phones, on page 180</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Voicemail settings are only visible in the Self Service interface if the user has a Voicemail box.</td>
<td>See Voicemail, on page 195</td>
</tr>
</tbody>
</table>
CHAPTER 9

Single Sign On

- SSO Certificate Management, page 79
- Configure Single Sign-On for Cisco Unified Communications Domain Manager, page 80

SSO Certificate Management

Use this procedure to create a self-signed or third-party-signed system certificate to use when setting up Single Sign-On (SSO) on the web proxy node on Cisco Unified Communications Domain Manager 10.6(1).

Procedure

Step 1 Login as hcsadmin.
Step 2 Select Single Sign On > Certificate Management.
Step 3 Click Add.
Step 4 On the Base tab, enter a Name and Description for the certificate.
   - For a self-signed certificate, leave Generate Certificate Signing Request unchecked.
   - For a third-party-signed certificate, check Generate Certificate Signing Request.
Step 5 For a self-signed certificate, control when the certificate is valid by changing the Valid From and Valid To fields. These are measured in seconds and default to 0 (now) and 315360000 (10 years), respectively.
Step 6 (Optional) Change the Key Length from the default of 1024.
Step 7 Click the Certificate Information tab.
Step 8 Complete the required fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>Enter the FQDN for your server.</td>
</tr>
</tbody>
</table>
Configure Single Sign-On for Cisco Unified Communications Domain Manager

Follow these steps to configure self-service Single Sign-On (SSO) for Cisco Unified Communications Domain Manager (Unified CDM). The configuration applies to the customers and customer administrators associated with the IdP.

SSO support for administrative users is defined as follows:

- SSO is not supported for administrative users under User Management > Local Admins because their passwords are stored locally (and so are not available for SSO).

- SSO is supported for administrative users under User Management > Users, except for users with the Role set to SelfService.

Before You Begin

Create a self-signed or third-party-signed system certificate before you configure self-service SSO. For more information, see SSO Certificate Management, on page 79.

The Unified CDM server and the IdP (identify provider) server must be configured so that their clocks are synchronized.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Code</td>
<td>A two-digit country code</td>
</tr>
<tr>
<td>State</td>
<td>An appropriate country subdivision</td>
</tr>
<tr>
<td>City</td>
<td>Your city</td>
</tr>
<tr>
<td>Organization</td>
<td>Your organization</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Your organization subunit</td>
</tr>
</tbody>
</table>

Step 9  Click Save.
Step 10 If you created a self-signed certificate you are done. If you requested a third-party-signed certificate, continue to the next step.
Step 11 Click the certificate you just created.
Step 12 Select Action > Export Certificate Request.
Step 13 Follow your organization's procedures to obtain the third-party signature for the certificate.
Step 14 Click the certificate.
Step 15 Select Action > Upload Signed Certificate.
Step 16 Browse to the signed certificate and click OK.
**Procedure**

**Step 1** Log in to Unified CDM as hcsadmin.

**Step 2** Select Single Sign On > SSO SP Settings.

**Step 3** Click Add.

*Note* Configure only one instance of SSO SP Settings.

**Step 4** On the Base tab, select the System Certificate to use. To allow the SSO SP Setting to expire, enter a number of hours in the Validity field.

*Note* Specifying an unsigned third-party-signed certificate will result in an error.

**Step 5** On the SAML SP Settings Tab, enter the FQDN of the Unified CDM server. Check **Sign Authn Requests** and **Want Assertions Signed** as required by your security environment.

**Step 6** Click Save.

**Step 7** To view the location of the Unified CDM SP metadata that you will upload to the IdP, select Single Sign On > SSO SP Metadata. Point your browser to the URL shown here, and then save a copy of the SP metadata.

**Step 8** Upload the SP metadata to the IdP.

*Note* The IdP must release the UID and map it to an appropriate attribute. For example, an IdP that authenticates with Active Directory can map the uid SAML attribute to sAMAccountName in the Active Directory server.

**Step 9** Download the IdP metadata from the IdP server.

*Note* The IdP must release the UID and map it to an appropriate attribute. For example, an IdP that authenticates with Active Directory can map the uid SAML attribute to sAMAccountName in the Active Directory server.

**Step 10** Log in as Provider, Reseller, or Customer Admin, depending on your IdP configuration level.

**Step 11** Select Administration Tools > File Management and upload the IdP metadata.

**Step 12** Select Single Sign On > SSO Identity Provider.

**Step 13** Click Add to add the SSO Identity Provider configuration.

*Note* Only one instance of an SSO Identity Provider can be configured for a hierarchy node.

**Step 14** Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Id</td>
<td>Entity ID of the IdP. This can be extracted from the IdP metadata file. This field is mandatory.</td>
</tr>
<tr>
<td>Login URI</td>
<td>Login URI for the IdP. This is the URI that will be imbedded in SSO Login URL. It can contain only alphanumeric characters and forward slashes. This field is mandatory.</td>
</tr>
<tr>
<td>Local Metadata File</td>
<td>Choose the IdP metadata file. This field is mandatory and must be unique across the system.</td>
</tr>
</tbody>
</table>
Check to enable SSO for users synched in or created at the current hierarchy level. Unchecking this node will disable SSO for the users associated with the defined IdP.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO Enabled</td>
<td>Check to enable SSO for users synched in or created at the current hierarchy level. Unchecking this node will disable SSO for the users associated with the defined IdP.</td>
</tr>
<tr>
<td>Note</td>
<td>Reminder to upload the IdP metadata file</td>
</tr>
<tr>
<td>SSO Login URL</td>
<td>Read-only field displays the SSO Login URL to use.</td>
</tr>
</tbody>
</table>

**Step 15** Click **Save** to save the SSO Identity Provider Configuration and enable SSO if selected.

**Step 16** Select **Single Sign On > SSO User** to display enabled SSO users.

Use this URL for your SSO login: https://<cucdm hostname>/sso/<login_URI>/login
Entitlement Management

- Entitlement Enforcement, page 83
- Entitlement Workflow, page 85
- Add Device Type, page 85
- Create Device Group, page 85
- Create an Entitlement Catalog, page 86
- Create an Entitlement Profile, page 87

Entitlement Enforcement

Service Levels

The following table shows the impact to a user when a service is disabled in the entitlement profile applied to the user.

<table>
<thead>
<tr>
<th>Service disabled</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Adding a phone to a user in Subscriber Management will fail. For an existing user with a phone, updates to the user in Subscriber Management will fail after an entitlement profile with Voice disabled is applied to the user.</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Adding Voicemail to a user in Subscriber Management will fail. For an existing user with Voicemail, updates in Subscriber Management will fail after an entitlement profile with Voicemail disabled is applied to the user.</td>
</tr>
</tbody>
</table>

Note

An entitlement profile can be explicitly assigned to a user, or implicitly applied if an entitlement profile is designated as the default entitlement profile in a hierarchy node at or above the user's hierarchy node.
<table>
<thead>
<tr>
<th>Service disabled</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence</td>
<td>Enabling Cisco Unified Communications Manager IM and Presence Service for a user in Subscriber Management will fail. For an existing user with Cisco Unified Communications Manager IM and Presence Service enabled, updates in Subscriber Management will fail after an entitlement profile with Presence disabled is applied to the user.</td>
</tr>
<tr>
<td>Extension Mobility</td>
<td>Adding Extension Mobility to a user in Subscriber Management will fail. For an existing user with Extension Mobility, updates in Subscriber Management will fail after an entitlement profile with Extension Mobility disabled is applied to the user.</td>
</tr>
<tr>
<td>Single Number Reach</td>
<td>For a new user, adding Single Number Reach in Subscriber Management will fail, and for an existing user with <strong>Enable Mobility</strong> checked, adding Single Number Reach will fail after an entitlement profile with Single Number Reach disabled is applied to the user.</td>
</tr>
</tbody>
</table>

**Device Groups**

A user to whom an entitlement profile is applied is limited to devices in the device groups assigned in the entitlement profile. Adding a Phone to a user in Subscriber Management will fail if the added Phone is not in a device group assigned to the entitlement profile applied to the user.

**Device Limits**

A user to whom an entitlement profile is applied is subject to the following device limits set in the entitlement profile:

- Total number of devices
- Total number of devices in a device group

Adding a Phone to a user in Subscriber Management will fail if the total number of devices limit or the total number of devices in a device group limit is exceeded.

**Transaction Log**

The transaction log messages contain detailed information that can be used to determine what entitlement profile limitation caused an action to fail.
Entitlement Workflow

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>(Optional) Define additional device types.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create device groups to define sets of device types that users may be entitled to.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create entitlement catalogs to define limits on devices and services that entitlement profiles may entitle users to.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create entitlement profiles to define the devices and services users are entitled to.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Identify the entitlement profile for users synced from Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Identify the entitlement profile for users synced from LDAP.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Assign entitlement profiles to existing users in Cisco Unified Communications Domain Manager 10.6(1).</td>
</tr>
</tbody>
</table>

Add Device Type

Cisco Unified Communications Domain Manager 10.6(1) is prepopulated with a list of current product types. However, the provider admin may add additional device types as needed.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Login as provider admin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>Entitlement &gt; Device Types</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the new device type.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

The new device type is added to the list of available device types that can be assigned to a device group.

Create Device Group

Device groups are used to limit entitlement to a defined subset of available device types.
Create an Entitlement Catalog

Entitlement catalogs limit the capabilities of entitlement profiles defined at hierarchy nodes at the same level or below where the entitlement catalog is defined.

Entitlement catalogs can be defined at the provider, reseller, or customer hierarchy level. Only one entitlement catalog may be defined at a given hierarchy node.

Procedure

Step 1 Log in as the provider administrator.
Step 2 Set the hierarchy path to the location where you want to create the entitlement catalog.
Step 3 Select Entitlement > Catalogs.
Step 4 Click Add.
Step 5 Enter a name and optional description for the entitlement catalog.
Step 6 Check the services to include in the entitlement catalog.
   The available services are Voice, Voicemail, Presence, Extension Mobility, and Single Number Reach.
Step 7 Specify the maximum number of devices allowable for the entitlement catalog.
   The maximum number cannot exceed the total of the maximums for all of the device groups included in the entitlement catalog.
Step 8 Select a Device Group to include in the entitlement catalog.
Step 9 For the selected device group, specify the maximum number of device allowed.
   The maximum number for any device group cannot exceed the maximum number of devices for the catalog.
Step 10 Click + to add additional device groups to the entitlement catalog.
Step 11 Click Save.

The entitlement catalog is created. Entitlement profiles can now be created at or below the level of the entitlement catalog.
Create an Entitlement Profile

Entitlement Profiles are used to define the services and devices a user is entitled to. An Entitlement Profile can be assigned to a user in the following situations:

- When the user is synched into Cisco Unified Communications Domain Manager 10.6(1) from LDAP.
- When the user is synched into Cisco Unified Communications Domain Manager 10.6(1) from Cisco Unified Communications Manager.
- When the user is created in Cisco Unified Communications Domain Manager 10.6(1) via the GUI, API, or bulk load.
- When the user is modified in Cisco Unified Communications Domain Manager 10.6(1).

Note

The maximum number of devices and maximum number of devices in a group are limitations for an individual user, not for all users in the system.

Before You Begin

An Entitlement Catalog must be defined at a hierarchy node at the same level as or above the hierarchy node where the Entitlement Profile is to be created. The Entitlement Catalog restricts the service and devices that can be entitled in the Entitlement Profile. An Entitlement Profile can further restrict services and devices a user is entitled to, but it cannot expand the services and devices beyond the restrictions defined in the Entitlement Catalog.

Procedure

Step 1 Log in as the provider administrator.
Step 2 Set the hierarchy path to the location where you want to create the Entitlement Profile.
Step 3 Select Entitlement > Profiles.
Step 4 Click Add.
Step 5 Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Entitlement Profile name. This field is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the entitlement Profile</td>
</tr>
<tr>
<td>Default Profile</td>
<td>Check to make this the default Entitlement Profile for the hierarchy node. Any previously-designated User Entitlement Profile will automatically have this field toggled off.</td>
</tr>
<tr>
<td>Voice</td>
<td>Check to entitle voice services.</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Check to entitle voicemail services.</td>
</tr>
</tbody>
</table>
### Create an Entitlement Profile

#### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence</td>
<td>Check to entitle presence services.</td>
</tr>
<tr>
<td>Extension Mobility</td>
<td>Check to entitle Extension Mobility services.</td>
</tr>
<tr>
<td>Single Number Reach</td>
<td>Check to entitle Single Number Reach service.</td>
</tr>
<tr>
<td>Maximum Number of Devices</td>
<td>Specify the maximum number of devices allowable for the Entitlement Profile. This field is mandatory. The maximum number cannot exceed the total of the maximums for all of the device groups included in the Entitlement Profile.</td>
</tr>
<tr>
<td>Device Group</td>
<td>Select a Device Group to include in the Entitlement Profile. This field is mandatory.</td>
</tr>
<tr>
<td>Maximum Number of Devices in Group</td>
<td>For the selected device group, specify the maximum number of devices allowed. This field is mandatory. The maximum number for any device group cannot exceed the maximum number of devices for the profile.</td>
</tr>
</tbody>
</table>

#### Step 6
Click + to add additional device groups to the Entitlement Profile.

#### Step 7
Click **Save**.

The Entitlement Profile is defined and can be assigned to users.
Dial Plan Management

- Dial Plan Example Workflow, page 90
- Create a Customer Dial Plan, page 90
- Create a Site Dial Plan, page 91
- Configure Class of Service, page 93
- Clone a Class of Service, page 96
- Configure Short Code, page 96
- Number Management, page 97
- Configure Cisco Unified Communications Manager Translation Patterns, page 109
- Clone Cisco Unified Communications Manager Translation Patterns, page 121
- Configure Cisco Unified Communications Manager Route Patterns, page 122
- Clone Cisco Unified Communications Manager Route Patterns, page 135
- Configure Directory Number Routing, page 136
- Provision Emergency Calls, page 137
- Configure SIP Trunks, page 138
- Delete SIP Trunks, page 162
- Clone SIP Trunks, page 162
- Reset SIP Trunks, page 163
- Restart SIP Trunks, page 163
- Configure Route Groups, page 164
- Delete Route Groups, page 166
- Configure Route Lists, page 166
- Associate Local Route Groups to a Device Pool, page 168
- Load Balancing, page 169
Dial Plan Example Workflow

Dial plan procedures available in Cisco Unified Communications Domain Manager 10.6(1) are found in this section. However, additional procedures and more detailed information about dial plans can be found in Cisco Hosted Collaboration Solution, Release 10.6(1) Dial Plan Management Guide for Cisco Unified Communications Domain Manager, Release 10.6(1).

Procedure

Step 1 Apply customer dial plan at customer.
Step 2 Apply site dial plan at site.
Step 3 Optionally, configure Class of Service at site.
Step 4 Add Directory Number Inventory at customer.
Step 5 If not using Site Location Codes (that is, you have deployed a Type 4 Dial Plan), configure Directory Number Routing at site to enable intra- and inter-site calls.
Step 6 Edit Site Defaults as follows:
   a) On the Device Defaults tab, set the Default CUCDM Device CSS to an appropriate device Class of Service.
   b) On the Line Defaults tab, set the Default CUCM Line CSS to an appropriate line Class of Service.
Step 7 For offnet PSTN call configuration, see Cisco Hosted Collaboration Solution, Release 10.6(1) Dial Plan Management Guide for Cisco Unified Communications Domain Manager, Release 10.6(1).
Step 8 For user, phone, and line configuration, see Subscriber Management section in Cisco Hosted Collaboration Solution, Release 10.6(1) End-User Provisioning Guide.

Create a Customer Dial Plan

This procedure determines the type of Cisco HCS dial plan schema (Type 1 to 4) to be used, depending on how you fill in the form.

Note
You can have only one dial plan per customer. If you try to add a second dial plan, the dial plan will fail. Once you have created the customer dial plan, Enable CSS filtering is the only setting that you can modify.

Procedure

Step 1 Log in as the Customer Administrator or the Provider Administrator. For a list of the roles and tasks that can be done at each level, see Cisco Hosted Collaboration Solution Roles and Privileges, on page 44.
Step 2 Select Dial Plan Management > Customer > Dial Plan.
Step 3 Click Add to add a Customer Dial Plan.
Step 4 Perform one of the following:
• If a Site Location Code is required for this customer, click the Site-Location Code (SLC) based dial plan? box, OR
• If an SLC is not required, go to Step 8.

Step 5 Perform one of the following:
• To add an extension prefix for the dial plan, click the Use extension prefix? box. Enter the extension prefix in the form and go to Step 8.
• To add an ISP for the dial plan, click the Inter-Site Prefix required for inter-site dialing? box. Enter the Inter-Site Prefix (ISP). The ISP can be one digit in length.

Step 6 If the ISP should be included in the directory number, click the Is ISP included in directory number? box. If not, go to Step 8.
Step 7 If the ISP should be included as part of the Voice Mail ID, click the Is ISP included in Voice Mail ID? box. If not, go to the next step.
Step 8 Check Enable CSS filtering to filter the calling search spaces available when configuring a Subscriber, Phone, or Line, to site level Class of Service calling search spaces. Filtering is disabled by default, which results in all available Cisco Unified Communications Manager calling search spaces being available when configuring a Subscriber, Phone, or Line.
Step 9 Click Save to add the Customer Dial Plan you defined.

Note
The Customer ID is a unique, auto-generated, read-only number allocated to the customer. The Customer ID is particularly useful in shared deployments (where a cluster may be shared across multiple customers) to correlate specific elements to a customer. It appears in the Cisco Unified Communications Manager as a prefix to elements (for example Cu2Si7 identifies Customer 2, Site 7).

Note
The Cisco HCS dial plan schemas are configured such that the customer-level dial plan elements are not pushed to the Cisco Unified Communications Manager until the first site for the customer is deployed. Therefore, you will not see any dial plan elements provisioned on the Cisco Unified Communications Manager until at least one site is deployed for the customer. See Create a Site Dial Plan, on page 91.

Note
When adding lines (DNs) at the site level, you must remember to define your DNs appropriately (that is, you are responsible for using ISP+SLC+EXT if you deploy a Type 2 dial plan). Otherwise your inter/intra site calls won’t route. To define your directory numbers, refer to Add Directory Number Inventory, on page 100.

### Create a Site Dial Plan

A site dial plan does not get created automatically for a site when a site is created. Perform this procedure to associate a site dial plan with the site. After the first site for a specific customer is deployed, the customer-level dial plan elements are provisioned on Cisco Unified Communications Manager, followed by the site-specific dial plan elements. Each subsequent site only has site-specific dial plan elements to provision, so it takes less time to create. If there is more than one site for a customer, do not forget to apply the site dial plan to each site.
Create a Site Dial Plan

Step 13 of this procedure takes a few minutes to provision the site dial plan, especially for the first site.

Note Each site can have one site dial plan only.

Important You can not edit the site dial plan once it is created. If you need to change the site dial plan, delete the current site dial plan and create a new one.

Before You Begin

A site dial plan cannot be created until a customer dial plan is created for the customer. There are attributes that are defined in the customer dial plan that are needed when creating a site dial plan.

Procedure

Step 1 Log in as the Customer Administrator or Provider Administrator. For a list of the roles and tasks that can be done at each level, see Cisco Hosted Collaboration Solution Roles and Privileges, on page 44.

When adding a site dial plan, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to create a site dial plan at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

Step 2 Select Dial Plan Management > Site > Dial Plan.

Step 3 Click Add to add a Site Dial Plan.

Step 4 Modify External Breakout Number field if desired. This is the PSTN prefix that is used when deploying a country dial plan. For Cisco HCS Type 1 to 4 dial plan schemas, you deploy country dial plans at the customer level. The country dial plan is not pushed to Cisco Unified Communications Manager until the first site associated with a given country is deployed. For example, if a site is associated with the United States of America, and it is the first site dial plan being created for the USA, the US country dial plan is deployed as part of creating the site's dial plan. Default is 9. The External Breakout Number is one digit in length.

Note Cisco supports only one External Breakout Number for each country. For example, all sites within USA have the same External break out as the first site within USA.

Step 5 Enter the Site Location Code using a maximum of eight digits. The SLC must be unique across sites for a customer. If the Customer Dial Plan does not use SLCs, this field does not appear.

Step 6 Enter the Extension Length. Values can be 1 to 11. Default is 4; for example, 2000.

Note When adding DNs for a site, extension length is not currently enforced. Therefore, the administrator must be conscious of extension length when adding DNs for a particular site; otherwise DNs may not be dialable.

Step 7 Perform one of the following for sites without Inter-Site Prefixes (ISPs):

Note This field appears if your Customer Dial Plan does not use ISPs; for example HCS Type 3 dial plans (SLC, no ISP, DN=SLC+EXT)

• Click the Use extension prefix? box if your customer dial plan has an extension prefix defined and you would like this site to use the extension prefix, OR
If an Extension prefix is not defined in the customer dial plan for this site, go to the next step.

Step 8 Enter the Area Code. Enter zero or more valid local area codes for the site. You must specify the length of the subscriber part of the PSTN number for each area code. This is used to generate the PSTN local route patterns for the site. For example, in the USA, if area codes are added for Dallas, Texas, the area codes could be specified for local dialing as 214, 469, and 972 with a subscriber length of 7.

Step 9 Enter the Local Number Length. This is the length for the subscriber section of the entire E.164 number.

Step 10 Click the Area Code used for Local Dialing box if the area code is needed for local dialing from this site. In the US this would determine whether you use 7 or 10 digit local dialing.

Step 11 Enter the Published number for the site. The site published number is the default E.164 mask when a line is associated to a phone at a particular site.

Step 12 Enter the Emergency Call Back Number for the site. The site emergency call back number is the calling number when initiating an outgoing emergency call. It can be used when a user is using extension mobility and making an emergency call from a site other than their own. It can be used when the emergency call goes out to the PSTN network, when the system includes the site emergency number so that the origin of the call is known. The system adds this calling party transformation to the DN2DDI4Emer-PT partition.

Note The Emergency Number is not the number to dial for an emergency. Instead, it is the number used to identify the calling party for emergency calls originating from a particular site.

Note Under the Emergency Number field, there is the Site ID read-only field. The Site ID is a unique, auto generated, read-only number for each customer site which is prefixed to elements as an identifier (for example Cu4Si2 indicates Customer 4, Site 2).

Step 13 Click Save to add the Site Dial Plan you defined. The site information is loaded on the Cisco Unified Communications Manager, and is identifiable by its Customer ID, Site ID prefix.

Configure Class of Service

Use this procedure to create a new Calling Search Space (CSS) or edit an existing CSS that is tied to a site. The CSS can be used as a Class of Service (COS) for a device or line, or any of the other templates that rely on COS to filter different features.

Procedure

Step 1 Log in as the Provider, Reseller, or Customer Administrator.

When adding Class of Service, ensure that you select a valid site under the customer in the hierarchy node breadcrumb at the top of the view. If you attempt to add a Class of Service at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

Step 2 Select Dial Plan Management > Site > Class of Service.

Note There is one default Internal Calling Line Identification Presentation (CLIP) Class of Service that appears in the list. The default COS is provisioned automatically based on the criteria you selected when you added the site.

Step 3 Perform one of
• To add a Class of Service, click **Add**.

• To edit an existing Class of Service, choose the COS to be updated by clicking on its box in the leftmost column, then click **Edit**.

• To clone an existing Class of Service, choose the COS to be cloned by clicking on its box in the leftmost column, then click **Clone**.

**Step 4** Enter a unique name for the Class of Service in the **Class of Service Name** field. Try to make the name as descriptive as possible using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_). You can also make use of macros that are available in the system to create a Class of Service name. For a list of possible macros, refer to **Macros, on page 94**. Macros allow you to dynamically add site IDs, customer IDs, and other types of information to the CSS.

**Example:**
Cu1-24HrsCLIP-PT-{{macro.HcsDpSiteName}}

**Note** The actual CSS that is sent to the Cisco Unified Communications Manager (based on the macros entered) is mirrored in the **Actual Calling Search Space** field. For example, the macro example above changes to Cu1-24HrsCLIP-PT-SiteABC.

**Step 5** Add a description for the Class of Service in the Description field if desired.

**Step 6** Choose route partition members to include in the Class of Service by performing the following:
   a) Click + to add route partitions.
   b) From the pulldown menu, select a route partition member.
   c) Repeat this step as required until you have selected all desired members for this Class of Service.

**Note** To remove a member from the Class of Service, click –.

**Step 7** Click **Save** to add the Class of Service that you defined.

The new Class of Service appears in the table of Classes of Service and it can be edited or deleted as required.

---

### Macros

Macros can be used in Cisco Unified Communications Domain Manager 10.6(1) to dynamically add site IDs, customer IDs, and other types of information when customizing dial plan schemas and Class of Service. Macros increase ease of use and reduce error.

Macros are evaluated within the context of a particular hierarchy node based on the scope specified in the schema group binding (for example, site, customer, provider).

The correct syntax for a macro is the word "macro" followed by a period (.), followed by the Named Macro as shown in the table that follows. Add double curly brackets ({{ }}) around the entire macro combination. For example, {{ macro.HcsDpCustomerName }} is the macro combination created using the first Named Macro in the table.

The following table provides a list of Named Macros currently available. This list will be expanded as new macros become available.
Table 5: Macros Available in Cisco Unified Communications Domain Manager 10.6(1)

<table>
<thead>
<tr>
<th>Named Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HcsDpCustomerName</td>
<td>Name of the customer (as specified when you create your customer)</td>
</tr>
<tr>
<td>HcsDpCustomerId</td>
<td>Systemwide, unique internal customer ID generated when you create a customer</td>
</tr>
<tr>
<td>HcsDpSiteName</td>
<td>Name of the site (as specified when you create a site under a customer)</td>
</tr>
<tr>
<td>HcsDpSiteId</td>
<td>Systemwide, unique internal site ID generated when you create a site</td>
</tr>
<tr>
<td>HcsDpUniqueCustomerPrefixMCR</td>
<td>Default unique Cisco HCS customer prefix in the form ‘Cu{{ macro.HcsDpCustomerId }}’</td>
</tr>
<tr>
<td>HcsDpUniqueSitePrefixMCR</td>
<td>Default unique HCS site prefix in the form ‘Cu{{ macro.HcsDpCustomerId }}Si {{ macro.HcsDpSiteId }}’</td>
</tr>
<tr>
<td>HcsDpSiteCountryMCR</td>
<td>Returns the country associated with a specific site</td>
</tr>
<tr>
<td>HcsDpSiteCountryIso</td>
<td>Returns the ISO 3166-1 alpha-3 three-letter country code associated with the country that is associated with a specific site</td>
</tr>
<tr>
<td>HcsDpPstnBreakout</td>
<td>Returns the PSTN prefix digit for the country that is associated with a specific site</td>
</tr>
<tr>
<td>HcsDpSiteAreaCodeInLocalDialingMCR</td>
<td>Returns True if a specific site requires area code for local PSTN dialing</td>
</tr>
<tr>
<td>HcsDpSiteNatTrunkPrefixMCR</td>
<td>Return the national trunk prefix associated to a particular site</td>
</tr>
<tr>
<td>HcsDpDefaultSiteDevicePoolMCR</td>
<td>Default Cisco HCS site device pool Cisco Unified Communications Manager element name</td>
</tr>
<tr>
<td>HcsDpDefaultSiteLocationMCR</td>
<td>Default Cisco HCS site location Cisco Unified Communications Manager element name</td>
</tr>
<tr>
<td>HcsDpDefaultSiteRegionMCR</td>
<td>Default Cisco HCS site region Cisco Unified Communications Manager element name</td>
</tr>
</tbody>
</table>

The following macros can be used to loop through the area codes specific for a particular site when adding translation patterns:

<table>
<thead>
<tr>
<th>Named Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HcsDpSiteAreaCodeMCR</td>
<td>Returns list of area codes associated with a specific site</td>
</tr>
<tr>
<td>HcsDpSiteAreaCodeItem_AreaCodeMCR</td>
<td>Return the area code attribute from the area code list item</td>
</tr>
<tr>
<td>HcsDpSiteAreaCodeItem_LocLenMCR</td>
<td>Return the local number length attribute from the area code list item</td>
</tr>
</tbody>
</table>
Clone a Class of Service

Use this procedure to clone an existing Class of Service (CoS) to the same site hierarchy node with a new name.

Procedure

Step 1 Log in as provider, reseller, customer, or site administrator.
Note When cloning a Class of Service (CoS), ensure that you select a valid site under the customer in the hierarchy node breadcrumb at the top of the view. If you attempt to clone a Class of Service at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

Step 2 Select Dial Plan Management > Site > Class of Service.

Step 3 Choose the Class of Service to be cloned by clicking on its box in the leftmost column.

Step 4 Click Action > Clone.

Step 5 Enter a unique name for the Class of Service in the Class of Service Name field. Make the name as descriptive as possible using up to 50 alphanumeric characters, including spaces, period(s), hyphens (‐), and underscore characters (_).

Step 6 (Optional) Add a description for the Class of Service in the Description field.

Step 7 Click Save to save the new Class of Service.
Note You must save the cloned CoS to the same site hierarchy node as the original CoS. You cannot save the cloned Class of Service to a different site, or to a different hierarchy node.

The new Class of Service appears in the table of Classes of Service and it can be edited or deleted as required.

Configure Short Code

Use this procedure to configure short codes. Short codes are used for abbreviated dialing to other extensions and services.

Before You Begin

You must add a Site Dial Plan before configuring Short Code. Refer to Create a Site Dial Plan, on page 91.

Procedure

Step 1 Log in to the server as the Provider, Reseller, Customer, or Site Administrator.

When adding a Short Code, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to add a Short Code at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

Step 2 Select Dial Plan Management > Site > Short Code.

Step 3 Click Add to add a Short Code.

Step 4 Enter a short code in the Short Code field using up to 16 characters with the following format:
• The first character may be 0-9, or *.
• The last character may be 0-9, #, or the wildcard character X.
• All other characters may be 0-9, . (period), or the wildcard character X. Only one . (period) is allowed.

Example: *2.XXX

Step 5 From the Short Code Type dropdown menu, choose one of

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called Mask</td>
<td>The called mask maps to the short code. Valid entries include the digits 0 through 9; the international escape character +; and the wildcard character X. For example, a called mask of 567XXX using short code *2.123 converts to 567123.</td>
</tr>
<tr>
<td>Directory Number</td>
<td>The directory number maps to the short code. Valid entries are digits 0 through 9.</td>
</tr>
<tr>
<td>Pre-dot with Called Prefix</td>
<td>The called prefix maps to the short code</td>
</tr>
</tbody>
</table>

Step 6 Enter the value for the Short Code Type in the Value field.

Step 7 Check the Use Originator's Calling Search Space check box to indicate that the short code will use the originator's calling search space for routing a call rather than an explicit customer CSS. If the originating device is a phone, the originator's calling search space is a combination of the device calling search space configured on their phone and line calling search space configured on the originating line.

Step 8 Click Save to add the Short Code that you defined. The new Short Code appears in the table of Short Codes and it can be edited or deleted as required.

Number Management

E164 Inventory Management

E.164 Inventory Management provides Direct Dial-In (DDI)/Direct Inward Dialing (DID) mapping to Directory Numbers (DN) using translation patterns in the Cisco Unified Communications Domain Manager. The DDI-to-DN mapping allows you to route incoming PSTN calls to the appropriate internal directory number.

E.164 Inventory Management includes the ability to:

• Add, view, and delete E.164 number inventory
• Associate a range of E.164 numbers to a range of DNs
• View associated range of E.164 numbers to a range of Directory numbers
• Disassociate a range of E.164 numbers from a range of DNs
• Associate a range or set of E.164 numbers to a single DN
• Disassociate a range or set of E.164 numbers from a single DN
• View single Directory number associations

The E.164 inventory is available in the dropdown menus for Site Published Number and Emergency Number when creating a Site Dial Plan.

Add E164 Inventory

Use this procedure to define an inventory of E.164 numbers available to end users at a site.

Important
Each addition to the E.164 Inventory must contain a unique set of numbers. That is, you cannot assign the same number more than once (globally).

Procedure

Step 1 Login as provider, reseller, or customer admin.
Step 2 Set the hierarchy path to point to the customer for whom you are adding the E.164 inventory.
Step 3 Select Dial Plan Management > Number Management > Add E164 Inventory.
Step 4 Provide the following information:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>Select the customer site for which you are adding the E.164 inventory. This field is mandatory.</td>
</tr>
<tr>
<td>Starting Number</td>
<td>Enter the starting number of the range of E.164 numbers. The field is populated with + followed by the country code associated with the selected site. Append the rest of the starting number after the country code. This field is mandatory.</td>
</tr>
<tr>
<td>Ending Number</td>
<td>Enter the ending number of the range of E.164 numbers. The format is the same as the Starting Number. This field is optional. If not provided, the single E.164 Number specified in the Starting Number will be added. If provided, the range of E.164 Numbers is added: Starting Number – Ending Number, inclusive. A maximum of 1000 numbers can be added at a time.</td>
</tr>
<tr>
<td>Country Code</td>
<td>The country code associated with the site. This field is read only and is for your reference because the Starting Number field and Ending Number field must contain a valid country code or else the E.164 inventory items will not be added successfully.</td>
</tr>
</tbody>
</table>

Step 5 Click Save.
View E164 Number Inventory

Use this procedure to view the inventory of E164 numbers.

Procedure

**Step 1**  
Login as provider, reseller, customer, or site admin.

**Step 2**  
Set the hierarchy path to limit the scope of E.164 numbers being viewed.

**Step 3**  
Select Dial Plan Management > Number Management > E164 Inventory.
A table containing the following information is displayed:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E164 Number</td>
<td>The individual E.164 number in the inventory.</td>
</tr>
<tr>
<td>Associated Flag</td>
<td>Indicates the E.164 number has been associated with a Directory Number.</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>Indicates the hierarchy of the site the E.164 number was created for.</td>
</tr>
</tbody>
</table>

Delete E164 Numbers from Inventory

Use this procedure to delete numbers from the E.164 inventory.

**Note**  
You cannot delete E.164 numbers that are currently associated with a Directory Number.

Procedure

**Step 1**  
Login as provider, reseller, or customer admin.

**Step 2**  
Set the hierarchy path to limit the scope of E.164 numbers being deleted.

**Step 3**  
Select Dial Plan Management > Number Management > E164 Inventory.

**Step 4**  
Perform one or both of the following:

- To delete an individual number, click the number, then click Delete.
- To delete multiple E.164 numbers, click the checkbox next to each number you want to delete, then click Delete. Use column filtering to narrow and refine the list of items to select for a batch delete.

**Step 5**  
Click Yes in the confirmation window.
Add Directory Number Inventory

Use this procedure to add a single directory number (DN) or range of DNs for your customer. The DNs (extensions) you specify are validated against the Dial Plan type (Type 1 to 4). The extension length assigned to the site is enforced for site location code (SLC)-based dial plans. The maximum number of directory numbers you can add at a time is 1,000. For more information on Type 1 to Type 4 dial plans, see Directory Numbers, on page 102.

If you are a customer with multiple sites and are using a Type 4 dialing plan, ensure that the directory numbers you specify are unique across sites.

Note
This procedure only creates the DN inventory in Cisco Unified Communications Domain Manager 10.6(1). The numbers are not passed on to Cisco Unified Communications Manager.

Note
Directory numbers can only be added or deleted. You cannot edit the directory numbers once they are added. The usage and availability property for each DN is associated with a line or taken into use by a service.

Before You Begin
You must deploy a customer and/or site dial plan before performing this procedure.

Procedure

Step 1 Log in as the Provider, Reseller, or Customer Administrator.
Step 2 Select an available Customer from the hierarchy node breadcrumb at the top of the interface.
Step 3 Select Dial Plan Management > Number Management > Add Directory Number Inventory.
Step 4 From the Site dropdown menu, select the site for which you are adding directory numbers. Leave this field empty to add customer level directory numbers.
Note Customer level directory numbers can only be created for dial plans that do not use site location codes (flat dial plans). Attempting to create customer level directory numbers for site location code based dial plans result in an error instructing the administrator to specify a site when adding new DN inventory.

Step 5 Using the Extension Length, Site Location Code, and ISP read-only fields as a guide for the site, enter the first number for the DN range in the Starting Extension field.
Note For a Type 4 dial plan (no SLCs), the Starting and Ending Extension fields must contain no more than 16 digits each, including the + sign before the DN number, if used. For Types 1 to 3 dial plans, the Starting and Ending Extension fields must be less than or equal to the site Extension Length. If the Starting or Ending Extension field length is less than the site Extension Length, the DN number will be padded with zeroes until its length equals that of the site Extension Length.

Example:
If the Extension Length field shows four digits for a Type 3 Dial Plan, ensure that you enter a number containing four digits or less in the Starting Extension field. For example, DN 1234. If you enter DN 123, the extension number will be created as DN 0123.

**Step 6** (Optional) Using the Extension Length, Site Location Code, and ISP read-only fields as a guide for the site, enter the last number for the DN range in the Ending Extension field. If you are adding a single DN, the ending number is the same as the starting number.

**Note** The maximum number of directory numbers you can add is 1,000 at a time. If you need more than 1,000 directory numbers, repeat this procedure as required to add ranges.

**Step 7** Click Save to save the single DN or DN range.

**Note** You can verify that the directory number or numbers were added correctly by navigating to Dial Plan Management > Number Management > Directory Number Inventory.

---

### View Directory Number Inventory

Use this procedure to view the range of directory numbers that have been defined for a site.

**Procedure**

1. **Step 1** Log in as the Provider, Reseller or Customer Administrator.
2. **Step 2** Select an available site from the hierarchy node breadcrumb at the top of the interface.
3. **Step 3** Select Dial Plan Management > Number Management > Directory Number Inventory.

The list of all directory numbers (DNs) configured for the site appears. You can view the list of DN numbers or delete a DN number from this page. To filter the list of directory numbers, click the up arrow beside the title of the Internal Number column. Enter the Search String you want to locate, and all directory numbers that match the search string appear.

When a DN is first added to the inventory, the Used column is blank, and the Available column shows "true". The Used column changes to "true" when the DN is put into use when a line is created and associated to a phone or subscriber. The Available column indicates that the DN is put into use by a device or service that does not allow a shared line (for example, a Hunt Pilot).

**Note** Adding a new DN to inventory on Cisco Unified Communications Domain Manager 10.6(1) does not add a directory number on Cisco Unified Communications Manager until it is associated to a line on Cisco Unified Communications Domain Manager 10.6(1).

The Directory Number Inventory entries appear in other end-user provisioning tasks in Cisco Unified Communications Domain Manager 10.6(1) as described in the table that follows. For more information on provisioning each of these tasks, refer to Cisco Hosted Collaboration Solution, Release 10.6(1) End-User Provisioning Guide.

<table>
<thead>
<tr>
<th>Task</th>
<th>Cisco Unified Communications Domain Manager 10.6(1) Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lines</td>
<td>Subscriber Management &gt; Lines</td>
<td>When lines are added through phones and subscriber, line details can be modified. The DN for the line cannot be modified; if you attempt to change the DN assigned to the line, the operation will fail.</td>
</tr>
</tbody>
</table>
### Directory Numbers

The Cisco HCS dial plan enables the creation of directory numbers (Cisco Unified Communications Manager Internal DNs) with the following choices of characteristics:

<table>
<thead>
<tr>
<th>Task</th>
<th>Cisco Unified Communications Domain Manager 10.6(1) Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phones</td>
<td>Subscriber Management&gt; Lines&gt; Dirn&gt; Pattern</td>
<td>The Dirn&gt; Pattern contains a list of available directory numbers. DNs that are in use are marked as &quot;true&quot; in the Directory Number Inventory. Only available DNs are listed.</td>
</tr>
<tr>
<td>Subscribers</td>
<td>Subscriber Management&gt; Subscribers&gt; Lines&gt; Dirn&gt; Pattern</td>
<td>The Dirn&gt; Pattern contains a list of available directory numbers. DNs that are in use are marked as &quot;true&quot; in the Directory Number Inventory. Only available DNs are listed.</td>
</tr>
<tr>
<td>Quick Add Subscribers</td>
<td>Subscriber Management &gt; Lines &gt; Directory Number</td>
<td>The Directory Number list contains available directory numbers. DNs that are in use are marked as &quot;true&quot; in the Directory Number Inventory. Only available DNs are listed.</td>
</tr>
<tr>
<td>PLAR (Hotdial)</td>
<td>Subscriber Management &gt; PLAR (Hotdial)</td>
<td>DNs provisioned to lines are displayed in the Hotdial Destination Pattern list</td>
</tr>
<tr>
<td>Hunt Groups</td>
<td>Subscriber Management &gt; Hunt Groups&gt; Members&gt; Directory Number &gt;</td>
<td>DNs provisioned to lines are displayed in the Pattern list</td>
</tr>
<tr>
<td>Call Pickup Groups</td>
<td>Subscriber Management &gt; Call Pickup Groups &gt; Call Pickup Group &gt; Line</td>
<td>DNs provisioned to member lines are displayed in the Pattern list</td>
</tr>
</tbody>
</table>
Table 6: Dial Plan Classification

<table>
<thead>
<tr>
<th>Dial Plan Configuration Type</th>
<th>Site Location Code (SLC)</th>
<th>IDP (Inter Site Prefix (ISP))</th>
<th>IDP in DN</th>
<th>Extension Dialing Prefix (EDP)</th>
<th>Extension Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>unnecessary with ISP</td>
<td>SLC + Ext, No ISP in SLC</td>
</tr>
<tr>
<td>2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>unnecessary with ISP</td>
<td>ISP+SLC+Ext (ISP is part of SLC)</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes/No</td>
<td>SLC+Ext and no ISP, can be with or without EDP</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Not Applicable</td>
<td>Ext (Flat Dial Plan/no SLC)</td>
</tr>
</tbody>
</table>

The specific terminology used above is explained in detail in the sections that follow.

Delete Site Directory Numbers

Use this procedure to delete one or more directory numbers at a site. You can bulk delete all directory numbers at a site using this procedure, or you can delete all directory numbers at a site automatically when you delete the site.

Procedure

**Step 1** Log in at any level. Select an available site from the hierarchy node breadcrumb at the top of the view if you are not at the Site level.

**Step 2** Select Dial Plan Management > Number Management > Directory Number Inventory.

**Step 3** From the list of directory numbers, choose the directory number(s) to be deleted, by clicking on one or more boxes in the leftmost column. To bulk delete all directory numbers at the site, click the box at the top of the leftmost column. To filter the list of directory numbers, click the up arrow beside the title of the Internal Number column. Enter the Search String you want to locate for deletion.

**Step 4** Click Delete to delete the directory number(s).

**Step 5** From the popup window, click Yes to confirm the deletion. When the delete action is complete, the directory number(s) disappears from the list.

Associate Range of E164 Numbers to a Range of Directory Numbers

Use this procedure to associate a range of E.164 numbers with a range of Directory numbers (DN) at a site. These associations create Discard Digits Instruction (DDI) associations so that incoming PSTN numbers are routed to directory numbers.
Only DNs or E.164 numbers that are not currently associated are available for association.

**Procedure**

**Step 1** Login as provider, reseller, customer or site admin.

**Step 2** Set the hierarchy path to point to the site where a range of E.164 numbers is to be associated with a range of directory numbers.

**Step 3** Select **Dial Plan Management > Number Management > E164 Associations (N to N DN).**

**Step 4** Click **Add.**

**Step 5** Provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>Select one of the following ranges from the dropdown menu:</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The range values you select map to the mask value when the association translation pattern is created. For example, when 10 is selected, all E.164 numbers and directory numbers that end in 0 are listed because the mask affects all digits 0 through 9, so you can't start the mask on a non-zero number. Likewise, when 100 is selected, the E.164 number and DN end in two zeros; this results in a mask of XX.</td>
</tr>
<tr>
<td></td>
<td>• 1—To list all E.164 numbers and DNs</td>
</tr>
<tr>
<td></td>
<td>• 10—To list all E.164 numbers and DNs that end in one zero (0)</td>
</tr>
<tr>
<td></td>
<td>• 100—To list all E.164 numbers and DNs that end in two zeros (00)</td>
</tr>
<tr>
<td></td>
<td>• 1000—To list all E.164 numbers and DNs that end in three zeros (000)</td>
</tr>
</tbody>
</table>

This field is mandatory and affects what appears in the fields below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E164 Number</td>
<td>Select the starting number of the range of E.164 numbers from the dropdown menu. The field includes a + followed by the country code associated with the selected site, followed by the rest of the starting number after the country code. This field is mandatory.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN Number</td>
<td>Select the starting extension number from the dropdown menu. This field is mandatory.</td>
</tr>
</tbody>
</table>

**Step 6** Click **Save.**

A translation pattern is created on the Cisco Unified Communications Manager which is used to route inbound PSTN calls to their associated DN. This is the mapping between the E164 range and DN range.

---

**View Associated Range of E164 Numbers to a Range of Directory Numbers**

Use this procedure to view the ranges of E.164 numbers that are associated with a range of Directory numbers (DN).
Procedure

Step 1
Login as provider, reseller, customer, or site admin.

Step 2
Set the hierarchy path to the site where the E.164 numbers and Directory numbers are associated.

Step 3
Select Dial Plan Management > Number Management > E164 Associations (N to N DN).

A table containing the following information is displayed:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E164 Number</td>
<td>The starting E.164 number in the range</td>
</tr>
<tr>
<td>DN Number</td>
<td>The starting Directory number in the range</td>
</tr>
</tbody>
</table>

Range

One of the following:

- 1 — To indicate that a single E.164 number and DN are associated
- 10 — To indicate that a range of 10 numbers including the starting E.164 and starting DN are associated
- 100 — To indicate that a range of 100 numbers including the starting E.164 and starting DN are associated
- 1000 — To indicate that a range of 1000 numbers including the starting E.164 and starting DN are associated

Hierarchy

Indicates the hierarchy of the site where the E.164 number range and DN range association was created

Disassociate Range of E164 Numbers from a Range of Directory Numbers

Use this procedure to disassociate a range of E.164 numbers from a range of Directory numbers (DN).

Procedure

Step 1
Login as provider, reseller, customer, or site admin.

Step 2
Set the hierarchy path to the site where the E.164 numbers and Directory numbers are associated.

Step 3
Select Dial Plan Management > Number Management > E164 Associations (N to N DN).

An E164 Associations (N to N DN) table containing the following information is displayed:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E164 Number</td>
<td>The starting E.164 number in the range</td>
</tr>
<tr>
<td>DN Number</td>
<td>The starting DN number in the range</td>
</tr>
</tbody>
</table>
### Associate Set of E164 Numbers to a Single Directory Number

Use this procedure to associate a set of E.164 numbers with a single Directory number (DN). For example, you may wish to associate a set of E.164 numbers for the Sales department with an Attendant's directory number.

**Note**

Only DNs or E.164 numbers that are not currently associated are available for association.
Procedure

**Step 1**
Login as provider, reseller, customer or site admin.

**Step 2**
Set the hierarchy path to point to the site where a set of E.164 numbers is to be associated with a single DN.

**Step 3**
Select Dial Plan Management > Number Management > E164 Associations (N to 1 DN).

**Step 4**
Click Add.

**Step 5**
From the DN Number dropdown menu, select a single extension number. This field is mandatory.

**Step 6**
In the E164 Ranges table, click + as required, to add multiple sets of E.164 numbers. The E.164 numbers do not need to be contiguous. Provide the following information for each association:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E164 Range</td>
<td>Select one of the following sets from the dropdown menu:</td>
</tr>
<tr>
<td></td>
<td>• 1—To list all E.164 numbers</td>
</tr>
<tr>
<td></td>
<td>• 10—To list all E.164 numbers that end in one zero (0)</td>
</tr>
<tr>
<td></td>
<td>• 100—To list all E.164 numbers that end in two zeros (00)</td>
</tr>
<tr>
<td></td>
<td>• 1000—To list all E.164 numbers that end in three zeros (000)</td>
</tr>
<tr>
<td>This field is mandatory and affects what appears in the field below.</td>
<td></td>
</tr>
<tr>
<td>E164 Number</td>
<td>Select the starting number of the set of E.164 numbers from the dropdown menu. The field includes a + followed by the country code associated with the selected site, followed by the rest of the starting number after the country code. This field is mandatory.</td>
</tr>
</tbody>
</table>

**Step 7**
Repeat the previous step as required until all E.164 associations for the single DN are complete.

**Step 8**
Click Save.

One or more translation patterns are created on the Cisco Unified Communications Manager that is used to route inbound PSTN calls to their proper DN. This is the mapping between the set of E.164 numbers and the single Directory number. When you associate a set of E.164 numbers to a single DN, multiple translation patterns are created; that is, each DN-to-E164 range association results in a translation pattern being created on Cisco Unified Communications Manager.

---

**View E164 Set-to-Single Directory Number Associations**

Use this procedure to view the sets of E.164 numbers that are associated with a single Directory number (DN).

**Procedure**

**Step 1**
Login as provider, reseller, customer, or site admin.

**Step 2**
Set the hierarchy path to the site where the Directory number and E.164 numbers are associated.

**Step 3**
Select Number Management > E164 Associations (N to 1 DN).

A table containing the following information is displayed:
Disassociate E164 Set from a Single Directory Number

Use this procedure to disassociate a set of E.164 numbers from a single directory number. When you disassociate a set of E.164 numbers from a single DN, multiple translation patterns are deleted; that is, each DN-to-E.164 set association results in a translation pattern being deleted from Cisco Unified Communications Manager.

Procedure

Step 1 Login as provider, reseller, customer, or site admin.
Step 2 Set the hierarchy path to the site where the E.164 numbers and Directory number is associated.
Step 3 Select Dial Plan Management > Number Management > E164 Associations (N to 1 DN).

An E164 Associations (N to 1 DN) table containing the following information is displayed:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN Number</td>
<td>The DN number</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>Indicates the hierarchy of the site where the E164 number range and DN</td>
</tr>
<tr>
<td></td>
<td>association was created</td>
</tr>
</tbody>
</table>

Step 4 Perform one of the following:

- To disassociate multiple associations at one time, click the check box in the leftmost column of the E164 Associations (N to 1 DN) table, beside the numbers to be disassociated. Click all that apply.
- To disassociate a single association, click on its row in the E164 Associations (N to 1 DN) table. The details about the association appear.

Step 5 Click Delete.
Step 6 From the popup, click Yes to confirm the disassociation, or click No to retain the association.

The translation pattern mapping between the E.164 set and the DN number is deleted from the Cisco Unified Communications Manager.
Migrate Translation Patterns for E164-to-DN Associations

If you manually configured the Translation Patterns in the E164 Lookup partition to associate E.164 numbers to directory numbers for DDI routing, Cisco recommends you use the E164-to-DN Association feature for Cisco Unified Communications Domain Manager 10.1(2) (Unified CDM) and later.

Use this procedure to migrate the existing Translation Patterns.

Procedure

Step 1 Log in to Unified CDM as a provider, reseller, or customer administrator.
Step 2 Add the appropriate E.164 inventory at Dial Plan Management > Number Management > Add E164 Inventory.
Step 3 View the E.164 number inventory: Dial Plan Management > Number Management > E164 Inventory.
Step 4 Verify that the selected DN inventory is available for association: Dial Plan Management > Number Management > Directory Number Inventory.
Step 5 Remove the previously added Translation Patterns: Device Manager > CUCM > Translation Pattern.
Step 6 Create the appropriate associations using the E164-to-DN Association feature: Dial Plan Management > Number Management > E164 Associations (N to N DN). These associations restore the appropriate Translation Patterns in the E164 Lookup partition for the selected customer.
Step 7 View the new Translation Pattern: Device Manager > CUCM > Translation Pattern.

Configure Cisco Unified Communications Manager Translation Patterns

Sometimes it may be necessary to update the default dial plan translation patterns that are deployed as part of the default dial plan schemas that are delivered with the Cisco Unified Communications Domain Manager 10.6(1) template package. For example, you may want to make your default national number translation patterns more restrictive. Also, additional translation patterns could be deployed that are specific to a customer deployment. For example, customer-specific blocking patterns could be added by an administrator that are not defined in the standard country dial plan schema.

Caution

The Cisco HCS default dial plan includes most common translation and route patterns and in most cases, should be added automatically when a customer dial plan, site dial plan, and voice mail service is provisioned. If you wish to update translation and route patterns using Cisco Unified Communications Domain Manager 10.6(1), you must have a full understanding of the Cisco HCS dial plan. Refer to the Cisco Hosted Collaboration Solution, Release 10.6(1) Dial Plan Management Guide for Cisco Unified Communications Domain Manager, Release 10.6(1) at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-1-1/model.html.

Use this procedure to update Cisco Unified Communications Manager translation patterns that are provisioned by the dial plan schema or to add new translation patterns from Cisco Unified Communications Domain Manager 10.6(1) that are not part of the standard dial plan package. For more information on Cisco Unified
Communications Manager translation patterns, refer to http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmcfg/CUCM_BK_C95ABA82_00_admin-guide-100/CUCM_BK_C95ABA82_00_admin-guide-100_chapter_0101100.html.

**Procedure**

**Step 1** Log in to Cisco Unified Communications Domain Manager 10.6(1) as the Provider, Reseller, or Customer admin.

**Step 2** Make sure the hierarchy path is set to the node where you want to add or edit the translation pattern.

**Step 3** Perform one of

- If you are logged in as the Provider or Reseller Administrator, select **Device Management > CUCM > Translation Patterns**.
- If you are logged in as the Customer Administrator, select **Device Management > Advanced > Translation Patterns**.

**Step 4** Perform one of

- To add a new translation pattern, click **Add**, then go to Step 5.
- To edit an existing translation pattern, choose the pattern to be updated by clicking on its box in the leftmost column of the **Translation Patterns** table, then click **Modify** to edit the selected translation pattern. Go to Step 6.

**Step 5** From the **CUCM** pulldown menu, select the hostname, domain name, or IP address of the Cisco Unified Communications Manager to which you want to add the translation pattern.

**Note** The CUCM pulldown menu only appears when a translation pattern is added; it does not appear when you edit a translation pattern.

**Important** If you are adding or editing a translation pattern at any hierarchy node above a site level, the only Cisco Unified Communications Managers that appear in the **CUCM** pulldown list are Cisco Unified Communications Managers that are located at the node where you are adding the translation pattern, and all Cisco Unified Communications Managers in hierarchies above the node where you are adding the translation pattern. If you are adding or editing a translation pattern at a site level, the Cisco Unified Communications Manager that appears in the **CUCM** pulldown list is the Cisco Unified Communications Manager in the site's Network Device List (NDL). If the site does not have an NDL, or the NDL at the site does not have a Cisco Unified Communications Manager, the pulldown list is empty and a translation pattern cannot be added to the site.

**Step 6** Enter a unique name for the translation pattern in the **Translation Pattern** field, or modify the existing name of the translation pattern if desired. You can include numbers and wildcards (do not use spaces), in the Translation Pattern field. For example, enter 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 +. This field is mandatory.

**Step 7** Enter a unique name for the route partition in the **Partition** field, or modify the existing name of the partition if desired. This field is mandatory.

**Step 8** Enter a description for the translation pattern and route partition in the **Description** field, if desired. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).

**Step 9** From the **Partition Definition** tab, modify the following fields as required.
Usethe Corresponding Cisco Unified Communications Manager Attribute information provided in the table to manually verify in the Cisco Unified Communications Manager GUI that fields have been mapped correctly.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Precedence</td>
<td>From the pulldown menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this translation pattern:</td>
</tr>
<tr>
<td>(Mandatory)</td>
<td>• Executive Override—Highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash Override—Second highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash—Third highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Fourth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Priority—Fifth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Routine—Lowest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Default—Does not override the incoming precedence level but rather lets it pass unchanged</td>
</tr>
<tr>
<td>Default: Default</td>
<td>Corresponding Unified Communications Manager Attribute: MLPP Precedence</td>
</tr>
</tbody>
</table>

<p>| Route Class             | From the pulldown menu, choose a route class setting for this translation pattern: |
| (Mandatory)             | • 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.Clear, then specify Data or Hotline as the Route Class. Default: Default |
|                         | Corresponding Unified Communications Manager Attribute: Route Class            |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Search Space (Optional)</td>
<td>From the pulldown menu, choose the calling search space for which you are adding a translation pattern, if necessary.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: Calling Search Space</td>
</tr>
<tr>
<td>Use Originator's Calling Search Space</td>
<td>To use the originator's calling search space for routing a call, check the Use Originator's Calling Search Space check box.</td>
</tr>
<tr>
<td>(Optional)</td>
<td>If the originating device is a phone, the originator's calling search space is a result of device calling search space and line calling search space.</td>
</tr>
<tr>
<td></td>
<td>Whenever a translation pattern chain is encountered, for subsequent lookups Calling Search Space is selected depending upon the value of this check box at current translation pattern. If you check the Use Originator's Calling Search Space check box at current translation pattern, then originator's Calling Search Space is used and not the Calling Search Space for the previous lookup. If you uncheck the Use Originator's Calling Search Space check box at current translation pattern, then Calling Search Space configured at current translation pattern is used.</td>
</tr>
<tr>
<td></td>
<td>Default: Unchecked</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: Use Originator's Calling Search Space</td>
</tr>
<tr>
<td>Block this pattern (Optional)</td>
<td>Indicates whether you want this translation pattern to be used for routing calls (such 8[2-9]XX) or for blocking calls.</td>
</tr>
<tr>
<td></td>
<td>Default: Unchecked (meaning translation pattern is used for routing calls)</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: Block this pattern</td>
</tr>
<tr>
<td>Block Reason (Optional)</td>
<td>If you click Block this pattern radio button above, you must choose the reason that you want this translation pattern to block calls. From the pulldown menu, choose one of</td>
</tr>
<tr>
<td></td>
<td>• No Error</td>
</tr>
<tr>
<td></td>
<td>• Unallocated Number</td>
</tr>
<tr>
<td></td>
<td>• Call Rejected</td>
</tr>
<tr>
<td></td>
<td>• Number Changed</td>
</tr>
<tr>
<td></td>
<td>• Invalid Number Format</td>
</tr>
<tr>
<td></td>
<td>• Precedence Level Exceeded</td>
</tr>
<tr>
<td></td>
<td>Default: No Error</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: &lt;entry box next to Block this pattern&gt;</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Provide Outside Dial Tone (Optional)       | 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.  
Default: Checked  
Corresponding Unified Communications Manager Attribute: Provide Outside Dial Tone |
| Urgent Priority (Optional)                 | 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.  
Default: Unchecked  
Corresponding Unified Communications Manager Attribute: Urgent Priority |
| Do Not Wait for Interdigit Timeout on Subsequent Hops (Optional) | When you check this check box along with the Urgent Priority check box and the translation pattern matches with a sequence of dialed digits (or whenever the translation pattern is the only matching pattern), Cisco Unified Communications Manager does not start the interdigit timer after it matches any of the subsequent patterns.  
Note Cisco Unified Communications Manager does not start the interdigit timer even if subsequent patterns are of variable length or if overlapping patterns exist for subsequent matches.  
Whenever you check the Do Not Wait For Interdigit Timeout On Subsequent Hops check box that is associated with a translation pattern in a translation pattern chain, Cisco Unified Communications Manager does not start the interdigit timer after it matches any of the subsequent patterns.  
Note Cisco Unified Communications Manager does not start interdigit timer even if subsequent translation patterns in a chain have Do Not Wait For Interdigit Timeout On Subsequent Hops unchecked.  
Default: Unchecked  
Corresponding Unified Communications Manager Attribute: Do Not Wait for Interdigit Timeout On Subsequent Hops |
| Route Next Hop By Calling Party Number (Optional) | 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.  
Default: Unchecked  
Corresponding Unified Communications Manager Attribute: Route Next Hop By Calling Party Number |

**Step 10** From the **Calling Party Transformations** tab, modify the following fields as required.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Calling Party's External Phone Number</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. Default: Default</td>
</tr>
<tr>
<td>Number Mask (Optional)</td>
<td>Corresponding Unified Communications Manager Attribute: Use Calling Party's External Phone Number Mask</td>
</tr>
<tr>
<td>Calling Party Transform Mask (Optional)</td>
<td>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. Default: None</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: Calling Party Transform Mask</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls) (Optional)</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 +. Note: The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: Prefix Digits (Outgoing Calls)</td>
</tr>
</tbody>
</table>
Cisco Unified Communications Manager uses calling line ID presentation/restriction (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 one of

- **Default**—Choose if you do not want to change calling line ID presentation.
- **Allowed**—Choose if you want Cisco Unified Communications Manager to allow the display of the calling number.
- **Restricted**—Choose 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, and for more information about call display restrictions, see topics related to call display restrictions in the *Cisco Unified Communications Manager System Guide*.

Default: Default

Corresponding Unified Communications Manager Attribute: Calling Line ID Presentation

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Line ID Presentation (Mandatory)</td>
<td>Cisco Unified Communications Manager uses calling line ID presentation/restriction (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 one of • Default—Choose if you do not want to change calling line ID presentation. • Allowed—Choose if you want Cisco Unified Communications Manager to allow the display of the calling number. • Restricted—Choose 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>. <strong>Note</strong> 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, and for more information about call display restrictions, see topics related to call display restrictions in the <em>Cisco Unified Communications Manager System Guide</em>. Default: Default Corresponding Unified Communications Manager Attribute: Calling Line ID Presentation</td>
</tr>
</tbody>
</table>
### Calling Name Presentation (Mandatory)

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 one of

- **Default**—Choose if you do not want to change calling name presentation.
- **Allowed**—Choose if you want Cisco Unified Communications Manager to allow the display of the calling name information.
- **Restricted**—Choose 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*.

Default: Default

Corresponding Unified Communications Manager Attribute: Calling Name Presentation

### Calling Party Number Type (Mandatory)

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

- **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 the shortened subscriber name.

Default: Cisco Unified Communications Manager

Corresponding Unified Communications Manager Attribute: Calling Party Number Type
### Description

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

- 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.

Default: Cisco Unified Communications Manager

 Corresponding Unified Communications Manager Attribute: Calling Party Numbering Plan

### Step 11

From the Connected Party Transformations tab, modify the following fields as required.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Connected Line ID Presentation (Mandatory) | 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 one of  
  • Default—Choose if you do not want to change the connected line ID presentation.  
  • Allowed—Choose if you want to display the connected party phone number.  
  • Restricted—Choose 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*.  
Default: Default  
Corresponding Unified Communications Manager Attribute: Connected Line ID Presentation |
| Connected Name Presentation (Mandatory) | 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 one of  
  • Default—Choose if you do not want to change the connected name presentation.  
  • Allowed—Choose if you want to display the connected party name.  
  • Restricted—Choose 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*.  
Default: Default  
Corresponding Unified Communications Manager Attribute: Connected Name Presentation |

**Step 12** From the **Called Party Transformations** tab, modify the following fields as required.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard Digits (Optional)</td>
<td>Choose the discard digits instructions that you want to be associated with this translation pattern. See topics related to discard digits instructions in the <em>Cisco Unified Communications Manager System Guide</em> for more information.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: Discard Digits</td>
</tr>
<tr>
<td>Called Party Transform Mask (Optional)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: Called Party Transform Mask</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls) (Optional)</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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The appended prefix digit does not affect which directory numbers route to the assigned device.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
<tr>
<td></td>
<td>Corresponding Unified Communications Manager Attribute: Prefix Digits (Outgoing Calls)</td>
</tr>
</tbody>
</table>
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

- 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.

Default: Cisco Unified Communications Manager

Corresponding Unified Communications Manager Attribute: Called Party Number Type

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</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
- 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.|

Default: Cisco Unified Communications Manager

Corresponding Unified Communications Manager Attribute: Called Party Number Type
Called Party Numbering Plan (Mandatory)

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

- 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.

Default: Cisco Unified Communications Manager

Corresponding Unified Communications Manager Attribute: Called Party Numbering Plan

### Step 13

Perform one of

- To save a new translation pattern, click **Save**.
- To save an updated translation pattern, click **Update**.

---

## Clone Cisco Unified Communications Manager Translation Patterns

Use this procedure to clone existing Cisco Unified Communications Manager translation patterns that are provisioned by the dial plan schema. For more information on Cisco Unified Communications Manager translation patterns, refer to [http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmcfg/CUCM_BK_C95ABA82_00_admin-guide-100/CUCM_BK_C95ABA82_00_admin-guide-100_chapter_0101100.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmcfg/CUCM_BK_C95ABA82_00_admin-guide-100/CUCM_BK_C95ABA82_00_admin-guide-100_chapter_0101100.html).
**Procedure**

**Step 1** Log into Cisco Unified Communications Domain Manager 10.6(1) as the Provider, Reseller, or Customer admin.

**Step 2** Make sure the hierarchy path is set to the node where you want to save the cloned translation patterns.

**Step 3** Perform one of

- If you logged in as the Provider or Reseller Administrator, select **Device Management > CUCM > Translation Patterns**.

- If you logged in as the Customer Administrator, select **Device Management > Advanced > Translation Patterns**.

**Step 4** From the list of translation patterns, choose the pattern to be cloned, by clicking on its box in the leftmost column.

**Step 5** Click **Action > Clone**.

**Step 6** On the **Partition Definition** tab, enter a unique name for one or both of the following fields:

- Modify the translation pattern in the **Translation Pattern** field. You can include numbers and wildcards (do not use spaces). For example, enter 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 +.

- Modify the route partition in the **Partition** field.

**Note** The **Translation Pattern** field and **Partition** field work together and the combination must be unique. For example, when you clone a translation pattern you can leave the pattern the same, but use a different route partition; as long as the translation pattern and partition combination is unique, the clone operation will be successful.

**Step 7** Enter a description for the new translation pattern and route partition in the **Description** field, if desired. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).

**Step 8** Modify fields in the **Partition Definition**, **Calling Party Transformations**, **Connected Party Transformations**, and **Called Party Transformations** tabs as required. For more information on field options and defaults, see **Configure Cisco Unified Communications Manager Translation Patterns**, on page 109.

**Step 9** Click + to save the cloned translation pattern.

**Step 10** Repeat Steps 4 to 10 as required to clone other translation patterns.

---

**Configure Cisco Unified Communications Manager Route Patterns**

Sometimes it may be necessary to update the default dial plan route patterns that are deployed as part of the default dial plan schemas that are delivered with the Cisco Unified Communications Domain Manager 10.6(1) template package.
The Cisco HCS default dial plan includes most common translation and route patterns and in most cases, should be added automatically when a customer dial plan, site dial plan, and voice mail service is provisioned. If you wish to update translation and route patterns using Cisco Unified Communications Domain Manager 10.6(1), you must have a full understanding of the Cisco HCS dial plan. Refer to the Cisco Hosted Collaboration Solution, Release 10.6(1) Dial Plan Management Guide for Cisco Unified Communications Domain Manager, Release 10.6(1) at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-1-1/model.html.

Use this procedure to update Cisco Unified Communications Manager route patterns that are provisioned by the dial plan schema or to add new route patterns from Cisco Unified Communications Domain Manager 10.6(1) that are not part of the standard dial plan package. For more information on the latest Cisco Unified Communications Manager route patterns, refer to http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to Cisco Unified Communications Domain Manager 10.6(1) as the Provider, Reseller, or Customer admin.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Make sure the hierarchy path is set to the node where you want to add or edit the route pattern.</td>
</tr>
</tbody>
</table>
| Step 3 | Perform one of  
• If you are logged in as the Provider or Reseller Administrator, select Device Management > CUCM > Route Patterns.  
• If you are logged in as the Customer Administrator, select Device Management > Advanced > Route Patterns. |
| Step 4 | Perform one of  
• To add a new route pattern, click Add, then go to Step 5.  
• To edit an existing route pattern, choose the pattern to be updated by clicking on its box in the leftmost column of the Route Patterns table, then click Modify to edit the selected pattern. Go to Step 6. |
| Step 5 | From the CUCM pulldown menu, select the hostname, domain name, or IP address of the Cisco Unified Communications Manager to which you want to add the route pattern.  
**Note** The CUCM pulldown menu only appears when a route pattern is added; it does not appear when you edit a route pattern.  
**Important** If you are adding or editing a route pattern at any hierarchy node above a site level, the only Cisco Unified Communications Manager that appear in the CUCM pulldown list are Cisco Unified Communications Manager that are located at the node where you are adding the route pattern, and all Cisco Unified Communications Manager in hierarchies above the node where you are adding the route pattern. If you are adding or editing a route pattern at a site level, the Cisco Unified Communications Manager that appears in the CUCM pulldown list is the Cisco Unified Communications Manager in the site's Network Device List (NDL). If the site does not have an NDL, or the NDL at the site does not have a Cisco Unified Communications Manager, the pulldown list is empty and a route pattern can not be added to the site. |
| Step 6 | Enter the route pattern in the Route Pattern field, or modify the existing route pattern if desired. This field is mandatory. Enter the route pattern, including numbers and wildcards (do not use spaces); for example, enter |
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 +.

**Step 7** If you want to use a partition to restrict access to the route pattern, choose the desired partition from the pulldown **Route Partition** menu. If you do not want to restrict access to the route pattern, choose <None> for the partition.

**Note** Make sure that the combination of route pattern, route filter, and partition is unique within the Cisco Unified Communications Manager cluster.

**Step 8** Enter a description for the route pattern and route partition in the **Description** field, if desired. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), or angle brackets (<>).

**Step 9** From the **Pattern Definition** tab, modify the following fields as required.

**Tip** Use the Corresponding Cisco Unified Communications Manager Attribute information provided in the table to manually verify in the Cisco Unified Communications Manager GUI that fields have been mapped correctly.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Precedence (Mandatory)</td>
<td>From the pulldown menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this route pattern:</td>
</tr>
<tr>
<td></td>
<td>• Executive Override—Highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash Override—Second highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash—Third highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Fourth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Priority—Fifth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Routine—Lowest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Default—Does not override the incoming precedence level but rather lets it pass unchanged</td>
</tr>
<tr>
<td>Default: Default</td>
<td>Corresponding Unified Communications Manager Attribute: MLPP Precedence</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Precedence (Mandatory)</td>
<td>From the pulldown menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this route pattern:</td>
</tr>
<tr>
<td></td>
<td>• Executive Override—Highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash Override—Second highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash—Third highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Fourth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Priority—Fifth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Routine—Lowest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Default—Does not override the incoming precedence level but rather lets it pass unchanged</td>
</tr>
<tr>
<td>Default: Default</td>
<td>Corresponding Unified Communications Manager Attribute: MLPP Precedence</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Precedence (Mandatory)</td>
<td>From the pulldown menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this route pattern:</td>
</tr>
<tr>
<td></td>
<td>• Executive Override—Highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash Override—Second highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash—Third highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Fourth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Priority—Fifth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Routine—Lowest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Default—Does not override the incoming precedence level but rather lets it pass unchanged</td>
</tr>
<tr>
<td>Default: Default</td>
<td>Corresponding Unified Communications Manager Attribute: MLPP Precedence</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Apply Call Blocking Percentage (Optional)</th>
<th>Check this checkbox 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>The <strong>Apply Call Blocking Percentage</strong> field gets enabled only if the MLPP level is immediate, priority, routine, or default. Default: Unchecked</td>
</tr>
<tr>
<td>Default: Unchecked</td>
<td>Corresponding Unified Communications Manager Attribute: Apply Call Blocking Percentage</td>
</tr>
</tbody>
</table>

**Tip** Use the Corresponding Cisco Unified Communications Manager Attribute information provided in the table to manually verify in the Cisco Unified Communications Manager GUI that fields have been mapped correctly.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Precedence (Mandatory)</td>
<td>From the pulldown menu, choose a Multilevel Precedence and Preemption (MLPP) service setting for this route pattern:</td>
</tr>
<tr>
<td></td>
<td>• Executive Override—Highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash Override—Second highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Flash—Third highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Immediate—Fourth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Priority—Fifth highest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Routine—Lowest precedence setting for MLPP calls</td>
</tr>
<tr>
<td></td>
<td>• Default—Does not override the incoming precedence level but rather lets it pass unchanged</td>
</tr>
<tr>
<td>Default: Default</td>
<td>Corresponding Unified Communications Manager Attribute: MLPP Precedence</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Call Blocking Percentage (Optional) | 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. Values between 0 and 99 are allowed.  
  **Note** Cisco Unified Communications Manager calculates the maximum number of low priority calls to be allowed through this route pattern based on the call blocking percentage that you set for this destination.  
  **Note** The Call Blocking Percentage field gets enabled only if the Apply Call Blocking Percentage checkbox is checked.  
  Default: None  
  Corresponding Unified Communications Manager Attribute: &lt;Entry box next to Apply Call Blocking Percentage&gt; |
| Route Class (Mandatory) | From the pulldown menu, choose a route class setting for this route pattern:  
  - 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.Clear, then specify Data or Hotline as the Route Class.  
  Default: Default  
  Corresponding Unified Communications Manager Attribute: Route Class |
| Route List (Mandatory if gateway or trunk is not specified) | Choose the route list for which you are adding a route pattern.  
  Default: None  
  Corresponding Unified Communications Manager Attribute: Gateway/Route List |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Gateway/Trunk (Mandatory if route list is not specified) | Choose the gateway or trunk list for which you are adding a route pattern.  
**Note** If the gateway is included in a Route Group, this pulldown menu does not display the gateway. When a gateway is chosen in the pulldown menu, Cisco Unified Communications Manager uses all the ports in the gateway to route or block this route pattern. This action does not apply for MGCP gateways.  
Default: Unchecked  
Corresponding Unified Communications Manager Attribute: Gateway/Route List |
| Block this pattern (Optional) | Indicates whether you want this route pattern to be used for routing calls (such as 8[2-9]XX) or for blocking calls.  
Default: Unchecked (meaning route pattern is used for routing calls)  
Corresponding Unified Communications Manager Attribute: Block this pattern |
| Block Reason (Optional)      | If you click Block this pattern radio button above, you must choose the reason that you want this route pattern to block calls. From the pulldown menu, choose one of  
- No Error  
- Unallocated Number  
- Call Rejected  
- Number Changed  
- Invalid Number Format  
- Precedence Level Exceeded  
Default: No Error  
Corresponding Unified Communications Manager Attribute: <entry box next to Block this pattern> |
| Call Classification (Mandatory) | Call Classification indicates whether the call that is routed through this route pattern is considered either off (OffNet) or on (OnNet) the local network. When adding a route pattern, if you uncheck the Provide Outside Dial Tone checkbox, you set Call Classification as OnNet.  
Default: OnNet  
Corresponding Unified Communications Manager Attribute: Call Classification |
| Allow Device Override (Optional) | When the checkbox 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.  
Default: Unchecked  
Corresponding Unified Communications Manager Attribute: Allow Device Override |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide Outside Dial Tone (Optional)</td>
<td>Leave this checkbox checked to provide outside dial tone. To route the call in the network, uncheck the checkbox.</td>
</tr>
<tr>
<td>Allow Overlap Sending (Optional)</td>
<td>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 checkbox 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 Client Matter Code (CMC) and Forced Authorization Code (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 checkbox, the system disables the Allow Overlap Sending checkbox. Default: Unchecked Corresponding Unified Communications Manager Attribute: Allow Overlap Sending</td>
</tr>
<tr>
<td>Urgent Priority (Optional)</td>
<td>If the dial plan contains overlapping patterns, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). Check this checkbox to interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately.                                                        Default: Unchecked Corresponding Unified Communications Manager Attribute: Urgent Priority</td>
</tr>
<tr>
<td>Require Forced Authorization Code (Optional)</td>
<td>If you want to use forced authorization codes with this route pattern, check this checkbox. 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 checkbox, you should uncheck the Require Forced Authorization Code checkbox. Default: Unchecked Corresponding Unified Communications Manager Attribute: Require Forced Authorization Code</td>
</tr>
<tr>
<td>Authorization Level (Mandatory)</td>
<td>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. Range is 0 to 255. Default: 0 Corresponding Unified Communications Manager Attribute: Authorization Level</td>
</tr>
</tbody>
</table>
Description
Option

If you want to use client matter codes with this route pattern, check this checkbox. 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 checkbox, you should uncheck the Require Client Matter Code checkbox.

Default: Unchecked

Corresponding Unified Communications Manager Attribute: <Entry box next to Authorization Level>

Step 10 From the **Calling Party Transformations** tab, modify the following fields as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Require Client Matter Code</strong> (Optional)</td>
<td>If you want to use client matter codes with this route pattern, check this checkbox. 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 checkbox, you should uncheck the Require Client Matter Code checkbox. Default: Unchecked Corresponding Unified Communications Manager Attribute: &lt;Entry box next to Authorization Level&gt;</td>
</tr>
<tr>
<td><strong>Use Calling Party's External Phone Number Mask</strong> (Optional)</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. <strong>Note</strong> 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. Default: Default Corresponding Unified Communications Manager Attribute: Use Calling Party's External Phone Number Mask</td>
</tr>
<tr>
<td><strong>Calling Party Transform Mask</strong> (Optional)</td>
<td>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. Default: None Corresponding Unified Communications Manager Attribute: Calling Party Transform Mask</td>
</tr>
<tr>
<td><strong>Prefix Digits (Outgoing Calls)</strong> (Optional)</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 +. <strong>Note</strong> The appended prefix digit does not affect which directory numbers route to the assigned device. Default: None Corresponding Unified Communications Manager Attribute: Prefix Digits (Outgoing Calls)</td>
</tr>
</tbody>
</table>
Cisco Unified Communications Manager uses calling line ID presentation/restriction (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 one of

- Default—Choose if you do not want to change calling line ID presentation.
- Allowed—Choose if you want Cisco Unified Communications Manager to allow the display of the calling number.
- Restricted—Choose 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.

Default: Default

Corresponding Unified Communications Manager Attribute: Calling Line ID Presentation

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Calling Line ID Presentation (Mandatory) | Cisco Unified Communications Manager uses calling line ID presentation/restriction (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 one of  
- Default—Choose if you do not want to change calling line ID presentation.  
- Allowed—Choose if you want Cisco Unified Communications Manager to allow the display of the calling number.  
- Restricted—Choose 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.  
Default: Default  
Corresponding Unified Communications Manager Attribute: Calling Line ID Presentation |

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Calling Name Presentation (Mandatory) | 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 one of  
- Default—Choose if you do not want to change calling name presentation.  
- Allowed—Choose if you want Cisco Unified Communications Manager to allow the display of the calling name information.  
- Restricted—Choose 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.  
Default: Default  
Corresponding Unified Communications Manager Attribute: Calling Name Presentation |
### Calling Party Number Type (Mandatory)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>• 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 the shortened subscriber name. Default: Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>Default</td>
<td>Corresponding Unified Communications Manager Attribute: Calling Party Number Type</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Calling Party Numbering</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</td>
</tr>
<tr>
<td>Plan (Mandatory)</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>

Default: Cisco Unified Communications Manager  
Corresponding Unified Communications Manager Attribute: Calling Party Numbering Plan

**Step 11** From the **Connected Party Transformations** tab, modify the following fields as required.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Connected Line ID Presentation (Mandatory) | 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 one of
• Default—Choose if you do not want to change the connected line ID presentation.
• Allowed—Choose if you want to display the connected party phone number.
• Restricted—Choose 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*.  
Default: Default  
Corresponding Unified Communications Manager Attribute: Connected Line ID Presentation |
| Connected Name Presentation (Mandatory) | 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 one of
• Default—Choose if you do not want to change the connected name presentation.
• Allowed—Choose if you want to display the connected party name.
• Restricted—Choose 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*.  
Default: Default  
Corresponding Unified Communications Manager Attribute: Connected Name Presentation |

**Step 12** From the **Called Party Transformations** tab, modify the following fields as required.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard Digits (Optional)</td>
<td>Choose the discard digits instructions that you want to be associated with this route pattern. See topics related to discard digits instructions in the <em>Cisco Unified Communications Manager System Guide</em> for more information. Default: None. Corresponding Unified Communications Manager Attribute: Discard Digits</td>
</tr>
<tr>
<td>Called Party Transform Mask (Optional)</td>
<td>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. Default: None. Corresponding Unified Communications Manager Attribute: Called Party Transform Mask</td>
</tr>
<tr>
<td>Prefix Digits (Outgoing Calls) (Optional)</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. Default: None. Corresponding Unified Communications Manager Attribute: Prefix Digits (Outgoing Calls)</td>
</tr>
</tbody>
</table>
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

- **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.

Default: Cisco Unified Communications Manager

Corresponding Unified Communications Manager Attribute: Called Party Number Type
### Clone Cisco Unified Communications Manager Route Patterns

Use this procedure to clone existing Cisco Unified Communications Manager route patterns that are provisioned by the dial plan schema. For more information on Cisco Unified Communications Manager route patterns, refer to [http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/9_1_1/ccmcfg/CUCM_BK_A34970C5_00_admin-guide-91/CUCM_BK_A34970C5_00_admin-guide-91_chapter_0100010.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/9_1_1/ccmcfg/CUCM_BK_A34970C5_00_admin-guide-91/CUCM_BK_A34970C5_00_admin-guide-91_chapter_0100010.html).

---

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Called Party Numbering Plan (Mandatory) | 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:  
  - 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.  
Default: Cisco Unified Communications Manager  
Corresponding Unified Communications Manager Attribute: Called Party Numbering Plan |

---

**Step 13** Perform one of

- To save a new route pattern, click **Save**.
- To save an updated route pattern, click **Update**.
**Configure Directory Number Routing**

Use this procedure to define Directory Number Routing. Directory Number Routing is a translation pattern that is put into the PreISR and ISR partitions to route intrasite and intersite calls to extensions (directory numbers). This is similar to the way site location codes (SLCs) are used as short codes for Type 1, 2, and 3 customer dial plans.

Typically, Directory Number Routing is used for Type 4 (flat dial plans) so that from a customer and site perspective, you can see which patterns are directory numbers because there are no SLCs available.
**Procedure**

**Step 1** Log in as the Provider, Reseller, Customer, or Site Administrator.

When adding Directory Number Routing, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to add Directory Number Routing at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

**Step 2** Select **Dial Plan Management > Site > Directory Number Routing**.

**Step 3** Click **Add** to add Directory Number Routing.

**Step 4** Enter a prefix in the **Directory Number Routing Prefix** field using up to 3 characters.

**Example:**
Enter 234

**Step 5** Enter a DN mask length in the **Directory Number Mask Length** field.

**Example:**
Enter 4. For this example, the Directory Number Routing would be 234XXXX, where XXXX is the mask.

**Step 6** Click **Save** to add the Directory Number Routing that you defined.

The new Directory Number Routing appears in the table and it can be edited or deleted as required.

---

**Provision Emergency Calls**

There is no additional provisioning that is necessary for emergency calls. In Cisco Unified Communications Domain Manager 10.6(1), 911 is provisioned as part of the United States country scheme, and 999/112 is provisioned as part of the United Kingdom country scheme. For more information, see **Emergency Handling**, on page 137.

**Procedure**

**Step 1** When you **Create a Site Dial Plan**, on page 91, enter the Emergency Number in the Emergency Number field. This is the Site Emergency Published Number; it is sent if the line that makes the emergency call does not have DDI. Then, if there is a callback, the Site Emergency Published Number is dialed.

**Step 2** Ensure that a Local Route group is set up with SLRG-Emer set to the Route group. Refer to **Associate Local Route Groups to a Device Pool**, on page 168.

---

**Emergency Handling**

Emergency handling is device-based. It uses the device pool local route group to handle call routing. When a phone has no Direct Inward Dial (DDI) or the phone has DDI but it is in a remote location, emergency handling uses the Site's Emergency number.

The implementation is as follows:
An Emergency partition is created for each site.

For Device-Based Routing (DBR), a DeviceDBR CSS is created and for Line Based Routing (LBR) an EmerCSS is created. Both CSSs are country and site specific and they contain the Emergency partition.

Emergency Number translation patterns are added to the emergency partition when a site dial plan is added. This translation pattern leverages the UseOriginatingCSS, prefixes the called number with **104 and the calling number is prefixed with *1*LRID* to uniquely identify the calling site.

An Emergency route pattern matching **104 is added to the emergency partition with the route list set to use the Device Pool Emergency Local Route Group.

**Figure 2: Emergency Calling**

---

**Configure SIP Trunks**

**Procedure**

**Step 1** Log in as the Provider, Reseller, or Customer Administrator.

**Step 2** Make sure the hierarchy path is set to the node where the Cisco Unified Communications Manager is configured.

**Step 3** Perform one of

- If you logged in as the Provider or Reseller Administrator, select **Device Management > CUCM > SIP Trunks**.
- If you logged in as the Customer Administrator, select **Device Management > Advanced > SIP Trunks**.

**Step 4** Perform one of

- To add a new SIP trunk, click **Add**, then go to Step 4.
To edit an existing SIP trunk, choose the SIP trunk to be updated by clicking on its box in the leftmost column, then click **Modify** to edit the selected SIP trunk. Go to Step 5.

**Step 5** From the **CUCM** pulldown menu, select the hostname, domain name, or IP address of the Cisco Unified Communications Manager to which you want to add the SIP trunk.

**Note** The **CUCM** pulldown menu only appears when a SIP trunk is added; it does not appear when you edit a SIP trunk.

**Important** The only Cisco Unified Communications Managers that appear in the **CUCM** pulldown list are Cisco Unified Communications Managers that are located at the node where you are adding the SIP trunk, and *all* Cisco Unified Communications Managers in hierarchies above the node where you are adding the SIP trunk. To provision a Cisco Unified Communications Manager server, refer to the "Installation Tasks" section of *Installing Cisco Unified Communications Manager*.

**Step 6** Enter a unique name for the new SIP trunk in the **Device Name** field, or modify the existing **Device Name** if desired.

**Step 7** From the **Device Information** tab, modify the following fields as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Name</strong> (Mandatory)</td>
<td>Enter a unique identifier for the trunk using up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only. Default value: None</td>
</tr>
</tbody>
</table>
| **Trunk Service Type** (Mandatory) | Select one of  
  - None—Choose this option if the trunk is not used for call control discovery, Extension Mobility Cross Cluster, or Cisco Intercompany Media Engine  
  - Call Control Discovery—Choose this option to enable the trunk to support call control discovery.  
  - 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.  
  - Intercompany Media Engine—Ensure that the Cisco IME server is installed and available before you configure this field.  
  - IP Multimedia Subsystem Service Control (ISC)—Choose this option to enable the trunk to support IP multimedia subsystem service control. Default value: None (Default) |
| **Description** (Optional)    | Enter a descriptive name for the trunk using up to 114 characters in any language, but not including double-quotes ("), percentage sign (%), ampersand (&), backslash (\), or angle brackets (<>). Default value: empty |
**Option** | **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.
Default value: Default

Common Device Configuration (Optional) | 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.
Default value: None

Call Classification (Mandatory) | 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.
Default value: Use System Default

Media Resource Group List (Optional) | 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.
Default value: None
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Location (Mandatory)** | 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. Select the appropriate location for this trunk:  
  - **Hub_None**—Specifies that the locations feature does not keep track of the bandwidth that this trunk consumes.  
  - **Phantom**—Specifies a location that enables successful CAC across intercluster trunks that use H.323 protocol or SIP.  
  - **Shadow**—Specifies a location for intercluster enhanced location CAC. Valid for SIP intercluster trunks (ICT) only.  
  Default value: Hub_None |
| **AAR Group (Optional)** | 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 is attempted. Default value: None |
| **Tunneled Protocol** | 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 RPID headers on the SIP gateway.  
  Default value: None |
| **QSIG Variant** | To display the options in the QSIG Variant drop-down list box, select QSIG from the Tunneled Protocol pulldown menu. This parameter specifies the protocol profile that is sent in outbound QSIG facility information elements. From the pulldown menu, select one of  
  - **No Changes**—Default. Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise.  
  - **Not Selected**  
  - **ECMA**—Select for ECMA PBX systems that use Protocol Profile 0x91  
  - **ISO**—Select for PBX systems that use Protocol Profile 0x9F  
  Default value: No Changes |
### Option | Description
--- | ---
ASN.1 ROSE OID Encoding | To display the options in the ASN.1 ROSE OID Encoding pulldown menu, choose QSIG from the Tunneled Protocol pulldown menu. This parameter specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations. From the pulldown menu, select one of
- **No Changes**—Keep this parameter set to the default value unless a Cisco support engineer instructs otherwise.
- **Not Selected**
- **Use Global Value ECMA**—If you selected the ECMA option from the QSIG Variant pulldown menu, select this option.
- **Use Global Value ISO**—If you selected the ISO option from the QSIG Variant pulldown menu, select this option.
- **Use Local Value**

Default value: No Changes

Packet Capture Mode | This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. From the pulldown menu, select one of
- **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.

Default value: None

Packet Capture Duration (Optional) | 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. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.

Default value: 0 (zero), Range is from 0 to 300 minutes
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Note</th>
<th>Default value: False (Unchecked)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Termination Point Required (Optional)</td>
<td>You can configure Cisco Unified Communications Manager SIP trunks to always use an Media Termination Point (MTP). Check this 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.</td>
<td>If the check box remains unchecked, Cisco Unified Communications Manager attempts 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, there is no need for MTP.</td>
<td></td>
</tr>
<tr>
<td>Retry Video Call as Audio (Optional)</td>
<td>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 using Automatic Alternate Routing (AAR) and route list or hunt list.</td>
<td>Default value: True (Checked)</td>
<td></td>
</tr>
<tr>
<td>Path Replacement Support (Optional)</td>
<td>This check box is relevant when you select QSIG from the Tunneled Protocol pulldown menu. This setting works with QSIG tunneling to ensure that non-SIP information gets sent on the leg of the call that uses path replacement.</td>
<td>Default value: False (Unchecked)</td>
<td></td>
</tr>
<tr>
<td>Transmit UTF-8 for Calling Party Name (Optional)</td>
<td>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.</td>
<td>The phone may display malformed characters if the two ends of the trunk are configured with user locales that do not belong to the same language group.</td>
<td>Default value: False (Unchecked)</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmit UTF-8 Names for QSIG APDU (Optional)</td>
<td>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. Default value: False (Unchecked)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unattended Port (Optional)</td>
<td>Check this check box if calls can be redirected and transferred to an unattended port, such as a voice mail port. Default value: False (Unchecked)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRTP Allowed (Optional)</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 check box, Cisco Unified Communications Manager prevents SRTP negotiation with the trunk and uses RTP negotiation instead. <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 still works but the keys 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. Default value: False (Unchecked)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consider Traffic on This Trunk Secure</td>
<td>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. From the pulldown menu, select one of • When using both sRTP and TLS • When using sRTP Only—Displays when you check the SRTP Allowed check box Default value: When using both sRTP and TLS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Route Class Signaling Enabled    | From the pulldown menu, enable or disable route class signaling for the port. Route class signaling communicates special routing or termination requirements to receiving devices. It must be enabled for the port to support the Hotline feature. From the pulldown menu, select one of  
  • Default—The device uses the setting from the Route Class Signaling service parameter  
  • Off—Enables route class signaling. This setting overrides the Route Class Signaling service parameter  
  • On—Disables route class signaling. This setting overrides the Route Class Signaling service parameter.  
  Default value: Default |
| Use Trusted Relay Point (Mandatory) | From the pulldown menu, enable or disable whether Cisco Unified Communications Manager inserts a trusted relay point (TRP) device with this media endpoint. 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. 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.  
  Select one of  
  • Default—The device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates  
  • Off—Disables 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—Enables 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.  
  Default value: Default |
| PSTN Access (Optional)           | 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.  
  Default value: True (Checked) |
Step 8 From the **Call Routing General** tab, modify the following fields as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run On All Active Unified CM Nodes (Optional)</td>
<td>Check this check box to enable the trunk to run on every node. Default value: False (Unchecked)</td>
</tr>
</tbody>
</table>

Remote-Party-ID (Optional)  
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. Default value: True (Checked)
### Asserted-Identity (Optional)

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 or not the SIP trunk sends the SIP Privacy header depends on the SIP Privacy configuration.

**Outgoing SIP Trunk Calls—P Headers**

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.

**Outgoing SIP Trunk Calls—SIP Privacy Header**

The SIP Privacy header gets used only when you check the Asserted Identity check box and when the SIP trunk sends either a Privacy-Asserted Identity (PAI) or Privacy Preferred Identity (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.

**Incoming SIP Trunk Calls—P Headers**

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.

**Incoming SIP Trunk Calls—SIP Privacy Header**

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 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.

**Note**

The Remote-party ID and Asserted Identity options represent independent mechanisms for communication of display-identity information.

Default value: True (Checked)
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asserted-Type</td>
<td>From the pulldown menu, select 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—Screening 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 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 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>Note These headers get sent only if the Asserted Identity check box is checked. Default value: Default</td>
</tr>
<tr>
<td>SIP Privacy</td>
<td>From the pulldown menu, select one of the following values to specify the type of SIP privacy header for SIP trunk messages to include:</td>
</tr>
<tr>
<td>(Mandatory)</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>Note These headers get sent only if the Asserted Identity check box is checked. Default value: Default</td>
</tr>
</tbody>
</table>

**Step 9** From the **Call Routing Inbound** tab, modify the following fields as required.
<table>
<thead>
<tr>
<th>Option</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 that are coming in to the SIP device. Choose the number of significant digits to collect, from 0 to 32, or choose 99 to indicate all digits. <strong>Note</strong> Cisco Unified Communications Manager counts significant digits from the right (last digit) of the number that is called. Default value: 99</td>
</tr>
</tbody>
</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. Select one of
  • Default—Allowed. Choose Default if you 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.
  • Restricted—Choose Restricted if you do not want Cisco Unified Communications Manager to send connected line information. **Note** Be aware that this service is not available when QSIG tunneling is enabled. Default value: Default |
| Connected Name Presentation           | 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. Select one of
  • Default—Allowed. Choose Default if you want Cisco Unified Communications Manager to send connected name information.
  • Restricted—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. Default value: Default |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Search Space (Optional)</td>
<td>From the pulldown menu, 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 pulldown menu 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. <strong>Note</strong> To set the maximum list box items, choose System &gt; Enterprise Parameters and choose CCMAadmin Parameters. Default value: None</td>
</tr>
<tr>
<td>AAR Calling Search Space (Optional)</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. Default value: None</td>
</tr>
<tr>
<td>Prefix DN (Optional)</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 +. Default value: None</td>
</tr>
<tr>
<td>Redirecting Diversion Header - Delivery Inbound (Optional)</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. Default value: False (Unchecked)</td>
</tr>
<tr>
<td>Incoming Calling Party - Prefix (Optional)</td>
<td>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 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. Default value: None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Incoming Calling Party - Strip Digits (Optional)</td>
<td>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. Default value: None</td>
</tr>
<tr>
<td>Incoming Calling Party - Calling Search Space (Optional)</td>
<td>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. Default value: None</td>
</tr>
<tr>
<td>Incoming Calling Party - Use Device Pool CSS (Optional)</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. Default value: True (Checked)</td>
</tr>
<tr>
<td>Incoming Called Party - Prefix (Optional)</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 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. <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 does not apply any prefix or strip digit functionality. Default value: None</td>
</tr>
<tr>
<td>Incoming Called Party - Strip Digits (Optional)</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. <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 in these windows, do not enter the word, Default, in the Prefix field. Default value: None</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Incoming Called Party - 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. Default value: None</td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
</tr>
<tr>
<td>Incoming Called Party - 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. Default value: True (Checked)</td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
</tr>
<tr>
<td>Connected Party Transformation CSS (Optional)</td>
<td>This setting is applicable only for inbound calls. This setting allows you to transform the connected party number on the device to display the connected number in another format, such as a DID or E164 number. Cisco Unified Communications Manager includes the transformed number in the headers of various SIP messages, including 200 OK and mid-call update and reinvite messages. Make sure that the Connected Party Transformation CSS that you choose contains the connected party transformation pattern that you want to assign to this device. <strong>Note</strong> If you configure the Connected Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation pattern used for Connected Party Transformation in a non-null partition that is not used for routing. Default value: None</td>
</tr>
<tr>
<td>Use Device Pool</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. Default value: True (Checked)</td>
</tr>
<tr>
<td>Connected Party Transformation CSS (Optional)</td>
<td></td>
</tr>
<tr>
<td>Use Device Pool</td>
<td></td>
</tr>
</tbody>
</table>

**Step 10** From the **Call Routing Outbound** tab, modify the following fields as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called Party Transformation CSS (Optional)</td>
<td>This setting allows you to send the transformed called party number in an INVITE message for outgoing calls made over SIP Trunk. 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. <strong>Note</strong> 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 CSS in a non-null partition that is not used for routing. Default value: None</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Use Device Pool Called Party Transformation CSS** (Optional) | 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.  
Default value: True (Checked) |
| **Calling Party Transformation CSS** (Optional) | This setting allows you to send the transformed calling party number in an INVITE message for outgoing calls made over a SIP Trunk. Also when redirection occurs for outbound calls, this CSS is used to transform the connected number that is sent from Cisco Unified Communications Manager side in outgoing reINVITE / UPDATE messages. 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** 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.  
Default value: None |
| **Use Device Pool Calling Party Transformation CSS** (Optional) | 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.  
Default value: True (Checked) |
| **Calling Party Selection** (Mandatory) | Choose the directory number that is sent on an outbound call. Select one of the following options to 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.  
Default value: Originator |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Calling Line ID Presentation | 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. Select one of  
  - Default—Allowed. Choose Default if you want Cisco Unified Communications Manager to send calling number information.  
  - Restricted—Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling number information.  
  Default value: Default |
| (Mandatory)                  |                                                                                                                                                                                                         |
| Calling Name                 | Cisco Unified Communications Manager used 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. Select one of  
  - Default—Allowed. Choose Default if you want Cisco Unified Communications Manager to send calling name information.  
  - Restricted—Choose Restricted if you do not want Cisco Unified Communications Manager to send the calling name information.  
  Note: This service is not available when QSIG tunneling is enabled.  
  Default value: Default |
| Presentation                 |                                                                                                                                                                                                         |
| (Mandatory)                  |                                                                                                                                                                                                         |
### Description

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 pulldown menu, select one of:

- **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.

- **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.

- **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.

#### Note

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 Communications Manager systems of Release 9.0 or greater, or between a Cisco Unified Communications Manager 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.

Default value: Deliver DN only in connected party

### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling and Connected Party Info Format (Mandatory)</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 pulldown menu, select one of:</td>
</tr>
<tr>
<td>Redirecting Diversion Header Delivery - Outbound (Optional)</td>
<td>Check this 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. Use Redirecting Number for voice-messaging integration only. If your configured voice messaging system supports Redirecting Number, check the check box. Default value: False (Unchecked)</td>
</tr>
</tbody>
</table>
Enter the pattern, from 0 to 24 digits that you want to use to format the Called 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 also enter the international escape character +.

Default value: None

Enter a caller name to override the caller name that is received from the originating SIP Device.

Default value: None

This check box is used to specify whether you will use the caller ID and caller name in the URI outgoing request. If you check this check box, the caller ID and caller name is used in the URI outgoing request. If you do not check this check box, the caller ID and caller name is not used in the URI outgoing request.

Default value: False (Unchecked)

From the SP Info tab, modify the following fields to as required.

This field specifies that the configured Destination Address is an SRV record.

Default value: False (Unchecked)
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Destination - Destination Address IPv4 (Mandatory) | The Destination Address IPv4 represents the remote SIP peer with which this trunk will communicate. The allowed values for this field are an IP address, a fully qualified domain name (FQDN), or DNS SRV record only if the Destination Address is an SRV field is checked.  
**Tip** For SIP trunks that can support IPv6 or IPv6 and IPv4 (dual stack mode), configure the Destination Address IPv6 field in addition to the Destination Address field.  
**Note** 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.  
**Note** 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.  
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.  
Default value: None |
| Destination - Destination Address IPv6 (Mandatory if Destination - Destination Address IPv4 field above is not completed) | 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:  
• A fully qualified domain name (FQDN)  
• A DNS SRV record, but only if the Destination Address is an SRV field is checked.  
SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk.  
If the remote end is a Cisco Unified Communications Manager cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster.  
**Tip** 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.  
Default value: None. If IPv4 field above is completed, this field can be left blank. |
| Destination - Destination port (Mandatory) | Choose the destination port. Ensure that the value that you enter specifies any port from 1024 to 65535, or 0.  
**Note** You can now have the same port number that is specified for multiple trunks.  
You do not need to enter a value if the destination address is a DNS SRV port. The default 5060 indicates the SIP port.  
Default value: 5060 |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort Order (Mandatory)</td>
<td>Indicate the order in which the prioritize multiple destinations. A lower sort order indicates higher priority. This field requires an integer value. Default value: Empty</td>
</tr>
</tbody>
</table>
| MTP Preferred Originating Codec (Mandatory)| Indicate the preferred outgoing codec by selecting one of:  
  • 711ulaw  
  • 711alaw  
  • G729/G729a  
  • G729b/G729ab  
Note 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. This field is used only when the MTP Termination Point Required check box is checked. Default value: 711ulaw                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| BLF Presence Group (Mandatory)             | Configure this field with the Presence feature. From the pulldown menu, select 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.  
  • Standard Presence group is configured with installation. Presence groups that are configured in Cisco Unified Communications Manager Administration also appear in the pulldown menu.  
  • Presence authorization works with presence groups to allow or block presence requests between groups.  
Tip 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. Default value: Standard Presence Group                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
<p>| SIP Trunk Security Profile (Mandatory)      | Select 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. Default value: Non Secure SIP Trunk Profile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rerouting Calling Search Space (Optional)</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). Calling Search Space also applies to 3xx redirection and INVITE with Replaces features. Default value: None</td>
</tr>
<tr>
<td>Out-Of-Dialog Refer Calling Search Space (Optional)</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). Default value: None</td>
</tr>
<tr>
<td>SUBSCRIBE Calling Search Space (Optional)</td>
<td>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 pulldown menu, 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 pulldown menu. If you do not select a different calling search space for the SIP trunk from the pulldown menu, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, configure a calling search space as you do all calling search spaces. Default value: None</td>
</tr>
<tr>
<td>SIP Profile (Mandatory)</td>
<td>From the drop-down list box, select the SIP profile that is to be used for this SIP trunk. Default value: Standard SIP Profile</td>
</tr>
</tbody>
</table>
### DTMF Signaling Method (Mandatory)

Select one of:

- **No Preference**—Cisco Unified Communications Manager picks 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 checkbox is checked), SIP trunk negotiates 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 (OOB) 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 negotiates both out-of-band and RFC2833 DTMF methods. As a result, two DTMF events are sent for the same DTMF keypress (one out of band and the other, RFC2833).

Default value: No Preference

### Normalization Script (Optional)

From the pulldown menu, choose the script that you want to apply to this trunk. To import another script, on Cisco Unified Communications Manager go to the SIP Normalization Script Configuration window (**Device > Device Settings > SIP Normalization Script**), and import a new script file.

Default value: None

### Normalization Script - Enable Trace (Optional)

Check this check box to enable tracing within the script or uncheck the 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.

Default value: False (Unchecked)

### Script Parameters (Optional)

Enter parameter names and values in the format **Param1Name=Param1Value; Param2Name=Param2Value** where **Param1Name** is the name of the first script parameter and **Param1Value** is the value of the first script parameter. Multiple parameters can be specified by putting semicolon after each name and value pair. Valid values include all characters except equal signs (=), semi-colons (;); and non-printable characters, such as tabs. You can enter a parameter name with no value.
### Recording Information

<table>
<thead>
<tr>
<th>Description</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter one of</td>
<td></td>
</tr>
<tr>
<td>• 0—None (default)</td>
<td>Recording Information (Optional)</td>
</tr>
<tr>
<td>• 1—This trunk connects to a recording-enabled gateway</td>
<td></td>
</tr>
<tr>
<td>• 2—This trunk connects to other clusters with recording-enabled gateways</td>
<td></td>
</tr>
</tbody>
</table>

### Step 12

From the **GeoLocation** tab, modify the following fields as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geolocation (Optional)</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>On Cisco Unified Communications Manager, 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>Default value: None</td>
</tr>
<tr>
<td>Geolocation Filter (Optional)</td>
<td>From the pulldown menu, choose a geolocation filter.</td>
</tr>
<tr>
<td></td>
<td>If you leave the &lt;None&gt; setting, no geolocation filter gets applied for this device.</td>
</tr>
<tr>
<td></td>
<td>On Cisco Unified Communications Manager, 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>Default value: None</td>
</tr>
<tr>
<td>Send Geolocation Information (Optional)</td>
<td>Check this check box to send geolocation information for this device.</td>
</tr>
<tr>
<td></td>
<td>Default value: False (Unchecked)</td>
</tr>
</tbody>
</table>

### Step 13

Perform one of

- To save a new SIP trunk, click **Save**.
- To save an updated SIP trunk, click **Update**.

The SIP trunk appears in the SIP trunk list. You can view the SIP trunk and its characteristics by logging in to the Cisco Unified Communications Manager where the SIP trunk was added, selecting **Device > Trunk**, and performing the **Find** operation. When you click on the name of the SIP trunk in the list, the trunk characteristics are displayed.

**Note** The SIP trunk is automatically reset on the Cisco Unified Communications Manager as soon as it is added. To reset the SIP trunk at any other time, perform **Reset SIP Trunks**, on page 163.
Delete SIP Trunks

Procedure

Step 1 Log in as the Provider/Reseller or Customer Administrator.
Step 2 Perform one of
  • If you logged in as the Provider/Reseller Administrator, select Device Management > CUCM > SIP Trunks.
  • If you logged in as the Customer Administrator, select Device Management > Advanced > SIP Trunks.
Step 3 From the list of trunks, choose the SIP trunk to be deleted, by clicking on its box in the leftmost column.
Step 4 Click Delete to delete the SIP trunk.
Step 5 From the popup window, click Yes to confirm the deletion.

Clone SIP Trunks

Use this procedure to copy the characteristics of a SIP trunk to one or more SIP trunks. The cloned SIP(s) can be associated with the same Cisco Unified Communications Manager instance as the original SIP trunk, or can be associated with another Cisco Unified Communications Manager.

Note

If you are cloning SIP trunks from one Cisco Unified Communications Manager to another Cisco Unified Communications Manager, check that the cloned Cisco Unified Communications Manager values are accurate. A cloned Cisco Unified Communications Manager may have invalid values, such as calling search spaces or locations.

Procedure

Step 1 Log in as the Provider/Reseller or Customer Administrator.
Step 2 Perform one of
  • If you logged in as the Provider or Reseller Administrator, select Device Management > CUCM > SIP Trunks.
  • If you logged in as the Customer Administrator, select Device Management > Advanced > SIP Trunks.
Step 3 From the list of trunks, choose the SIP trunk to be cloned, by clicking on its box in the leftmost column.
Step 4 Click Action > Clone.
Step 5 (Optional) From the CUCM pulldown menu, select a different hostname, domain name, or IP address of the Cisco Unified Communications Manager to which you want to add the SIP trunk.
**Important** The only Cisco Unified Communications Managers that appear in the CUCM pulldown list are Cisco Unified Communications Managers that are located at the hierarchy node where you added the original SIP trunk, or all nodes above it in the hierarchy. To provision a Cisco Unified Communications Manager server, refer to the “Installation Tasks” section of *Installing Cisco Unified Communications Manager*.

**Step 6** Enter a unique name for the new SIP trunk in the **Device Name** field.

**Step 7** Modify fields in the **Device Information**, **Call Routing General**, **Call Routing Outbound**, **SIP Info**, or **GeoLocation** tabs as required. For more information on field options and defaults, see *Configure SIP Trunks*, on page 138.

**Step 8** Click **Save** to save the cloned SIP trunk. The SIP trunk appears in the SIP trunk list. You can verify the SIP trunk and its characteristics by logging in to the Cisco Unified Communications Manager where the SIP trunk was added, selecting **Device > Trunk**, and performing the **Find** operation. When you click on the name of the SIP trunk in the list, the trunk characteristics are displayed.

**Step 9** Repeat Steps 3 to 8 to clone another SIP trunk if desired.

---

**Reset SIP Trunks**

Use this procedure to shut down a SIP trunk and bring it back into service. This procedure does not physically reset the hardware; it only reinitializes the configuration that is loaded by the Cisco Unified Communications Manager cluster. To restart a SIP trunk without shutting it down, use *Restart SIP Trunks*, on page 163.

**Procedure**

**Step 1** Log in as the Provider/Reseller or Customer Administrator.

**Step 2** Perform one of

- If you logged in as the Provider or Reseller Administrator, select **Device Management > CUCM > SIP Trunks**.

- If you logged in as the Customer Administrator, select **Device Management > Advanced > SIP Trunks**.

**Step 3** From the list of trunks, choose the SIP trunk to be reset, by clicking on its box in the leftmost column.

**Step 4** Click **Edit** to open the SIP trunk information.

**Step 5** Select **Action > Reset**.

---

**Restart SIP Trunks**

Use this procedure to restart a SIP trunk without shutting it down first. To shut down a SIP trunk prior to the reset, see *Reset SIP Trunks*, on page 163.
If the SIP trunk is not registered with Cisco Unified Communications Manager, you cannot restart it.

Restarting a SIP trunk drops all active calls that are using the trunk.

**Procedure**

**Step 1** Log in as the Provider/Reseller or Customer Administrator.

**Step 2** Perform one of:

- If you logged in as the Provider/Reseller Administrator, select Device Management > CUCM > SIP Trunks.
- If you logged in as the Customer Administrator, select Device Management > Advanced > SIP Trunks.

**Step 3** From the list of trunks, choose the SIP trunk to be restarted, by clicking on its box in the leftmost column.

**Step 4** Click **Edit** to open the SIP trunk information.

**Step 5** Select **Action > Restart**.

---

### Configure Route Groups

A route group allows you to designate the order in which gateways 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 that long distance calls to the less expensive carrier are given priority. Calls only route to the more expensive carrier if the first trunk is unavailable.

Use this procedure to add or modify route groups.

**Note**

Each gateway or gateway and port combination can only belong to one route group and can only be listed once within that route group. All gateways in a route group must have the same route pattern. The pattern is assigned to the route list containing the route group (not the route group itself).

Route groups are optional. If a proposed route group only contains one gateway or one gateway and port combination and that route group is not to be included in a route list, the route group is not needed.

**Before You Begin**

You must define one or more gateway or SIP trunks before you add a route group.

**Procedure**

**Step 1** Log in as the Provider/Reseller or Customer administrator.

**Step 2** Perform one of
If you logged in as the Provider or Reseller Administrator, select Device Management > CUCM > Route Groups.

If you logged in as the Customer Administrator, select Device Management > Advanced > Route Groups.

### Step 3
Perform one of
- To add a new route group, click Add.
- To edit an existing route group, choose the group to be updated by clicking on its box in the leftmost column, then click Update to edit the selected route group.

### Step 4
From the CUCM pulldown menu, select or modify the Cisco Unified Communications Manager that corresponds to the route group.

### Step 5
Enter a unique name for the new route group in the Route Group Name field, or modify the existing Route Group Name if desired. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, period(s), hyphens (-), and underscore characters (_). Ensure that each route group name is unique to the route plan.

**Tip** Use concise and descriptive names for the route group. 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.

### Step 6
From the pulldown menu, select or modify the Distribution Algorithm options for the route group. Default value is Circular.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Down</td>
<td>Select this option if you want Cisco Unified Communications Manager to distribute a call to idle or available members starting with the first idle or available member of a route group to the last idle or available member of a route group.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You need to select Top Down to prioritize the order of devices in Step 10.</td>
</tr>
<tr>
<td>Circular</td>
<td>Select this option if you want Cisco Unified Communications Manager to distribute a call to idle or available members starting from the (n+1)th member of a route group, where the nth member is the member to which the Cisco Unified Communications Manager most recently extended a call. If the nth member is the last member of a route group, Cisco Unified Communications Manager distributes a call starting from the top of the route group.</td>
</tr>
</tbody>
</table>

### Step 7
Click + to open the Members box. Perform one or more of the following steps:
- To add a device to the route group, perform Step 8.
- To modify the priority of a device, go to Step 10.
- To remove a device from the route group, go to Step 11.

### Step 8
To add a device to the route group, from the Device Name pulldown menu, choose the device where the route group is added.

**Note** When a SIP trunk or gateway is added, all ports on the device are selected.
Step 9  To add another device to the route group, click + at the top of the Members box, then repeat Steps 8 and 9 for each additional device.

Step 10 To change the priority of a device, move the device up or down in the list by clicking the arrows on the right side of the Members box. Using the Up arrow, move the device higher in the list to make it a higher priority in the route group, or using the Down arrow, move the device lower in the list to make it a lower priority in the route group.

Note The Top Down distribution algorithm must be selected in Step 6 to prioritize the order of devices.

Step 11 To remove a device from the route group, select the device in the Members box and click the – on the right side of the Members box.

Note You must leave at least one device in the route group.

Step 12 To save a new or updated route group, click Save. The route group appears in the Route Group list.

---

Delete Route Groups

Procedure

Step 1 Log in as the Provider/Reseller or Customer Administrator.

When deleting a route group, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to delete a route group at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

Step 2 Perform one of

- If you logged in as the Provider or Reseller Administrator, select Device Management > CUCM > Route Groups.

- If you logged in as the Customer Administrator, select Device Management > Advanced > Route Groups.

Step 3 From the list of trunks, choose the route group to be deleted, by clicking on its box in the leftmost column. The Route Group profile appears.

Step 4 Click Delete to delete the Route Group.

Step 5 From the popup window, click Yes to confirm the deletion.

---

Configure Route Lists

Route lists are made up of route groups and are associated with route patterns. A route list associates a set of route groups with a route pattern and determines the order in which those route groups are accessed. The order controls the progress of the search for available trunk 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.

Use the following procedure to add route lists or to add, remove or change the order of route groups in a route list.

**Before You Begin**

Configure route groups before performing this procedure.

**Procedure**

**Step 1** Log in to as the Provider/Reseller or Customer administrator.

**Note** When configuring a route list as a Provider or Reseller, ensure that you select a valid customer or site under your customer in the hierarchy node breadcrumb at the top of the view.

**Step 2** Perform one of

- If you logged in as the Provider or Reseller Administrator, select **Device Management > CUCM > Route Lists**.

- If you logged in as the Customer Administrator, select **Device Management > Advanced > Route Lists**.

**Step 3** Perform one of

- To add a new route list, click **Add**, then go to Step 4.

- To edit an existing route list, choose the list to be updated by clicking on its box in the leftmost column, then click **Edit** to update the selected route list. Go to Step 5.

**Step 4** From the **CUCM** pulldown menu, select a Cisco Unified Communications Manager for the route list.

**Step 5** Enter a unique name for the new route list in the **Name** field, or modify the existing route list **Name** if desired. The name can comprise up to 50 alphanumeric characters and can contain any combination of spaces, period(s), hyphens (-), and underscore characters (_). Ensure that each route list name is unique to the route plan.

**Tip** Use concise and descriptive names for the route list. 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.

**Step 6** Enter or modify the description for the route list in the **Description** field.

**Step 7** From the **Call Manager Group Name** pulldown menu, select a Cisco Unified Communications Manager Group. Default is the default field. You can choose from Default, None or select a group.

**Note** The route list registers with the first Cisco Unified Communications Manager in the group (which is the Primary Cisco Unified Communications Manager).

**Step 8** Perform one of

- To enable this route list, ensure that the **Route List Enabled** check box is checked (Default for a new route list).
• To disable this route list, uncheck the **Route List Enabled** check box. Calls in progress do not get affected, but this route list does not accept additional calls.

**Step 9**
To enable the active route list to run on every node, check the **Run On Every Node** check box.

**Step 10**
To add a route group to this route list, perform the following steps:
- a) Click `+` on the right side of the **Route Group Items** box.
- b) From the **Route Group Name** pulldown menu, select the route group.

**Step 11**
To remove a route group from this route list, click `–` on the right side of its row in the **Member** box.

**Step 12**
To change the priority of a route group, move it up or down in the list by clicking the arrows on the right side of the **Member** box. Using the Up arrow, move the group higher in the list to make it a higher priority, or using the Down arrow, move the group lower in the list to make it a lower priority.

**Step 13**
To save a new or updated route list, click **Save**.

---

**Associate Local Route Groups to a Device Pool**

Use this procedure to associate a local route group with an existing device pool for each site. This allows calls from a device that is tied to a device pool to go out on a specific route group based on the call type. You cannot use this procedure to add or delete device pools.

For example, you can associate multiple local route groups such as Emergency Route Group, Primary Local Route Group (for site A), Secondary Local Route Group (for site A), Primary Local Route Group (for site B), and Secondary Local Route Group (for site B). The Local Route Group feature enables you to specify different route groups for each site (site A and site B) for the respective device pool. Also, you can define a separate call routing option for emergency calls when you associate the Emergency Route Group with a different route group. Hence you can easily define separate call routing options for emergency calls and PSTN calls.

**Procedure**

**Step 1**
Log in to as the Provider/Reseller or Customer administrator.

When associating a local route group, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to associate a local route group at any other node in the hierarchy, a popup alerts you to select a site hierarchy node.

**Step 2**
Perform one of the following:
- If you logged in as the Provider or Reseller Administrator, select **Device Management > CUCM > Device Pools**.
• If you logged in as the Customer Administrator, select **Device Management > Advanced > Device Pools**.

**Step 3** Click the device pool to be associated.

**Step 4** From the **Cisco Unified CM Group** pulldown menu, select a specific Cisco Unified Communications Manager group or leave the **Cisco Unified CM Group** as Default.

**Step 5** Click the Local Route Group Settings tab.

**Step 6** In the grid, from the **Local Route Group** pulldown menu, select the local route group.

**Step 7** In the grid, from the **Route Group** pulldown menu, select the route group or gateway.

**Step 8** To save the new local route association, click **Save**.

---

### Load Balancing

Cisco Unified Communications Manager groups provide both call-processing redundancy and distributed call processing. You can distribute devices, device pools, and Cisco Unified Communications Managers among the groups to improve redundancy and load balancing in your system.

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. For example, Group 1 points to Device Pool 1, Group 2 points to Device Pool 2, and Group 3 points to Device Pool 3. 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.

Load balancing is a manual process on Cisco Unified Communications Manager requiring you to perform the following tasks:

1. Add new, custom Cisco Unified Communications Manager groups and device pools.
2. Synchronize the groups and device pools into Cisco Unified Communications Domain Manager.
3. Select the appropriate group and device pool in the Subscriber or Phone configuration for the site. To create more than one configuration for a site, create at least two Cisco Unified Communications Manager groups, then associate a device pool to the appropriate Cisco Unified Communications Manager group.

To determine if load balancing is required for your network, you can check the current device traffic load in Cisco Unified Communications Manager using the **System > Device Pool** menu path. When you click on the device configuration information for a specific device pool, the Device Pool Information field lists the number of members in the Device Pool. Compare different device pools to see if the members are evenly divided between pools.

To perform load balancing, see **Load Balancing Using Site Default Device Pool**, on page 170.
Load Balancing Using Site Default Device Pool

A default device pool is created for each site when the site dial plan is deployed for the Type 1 through 4 dial plan schema groups. This procedure uses the default site device pools, so you do not need to create any additional device pools directly on Cisco Unified Communications Manager. Perform this procedure to load balance using the default site device pool. In this procedure, the default device pool is updated to point to the appropriate Cisco Unified Communications Manager group.

Using this configuration, redundancy is gained within a site while load balancing is gained across multiple sites. Since there is one device pool per site, all devices at a site home to the same sequence of Cisco Unified Communications Managers, providing failover redundancy. Devices in different sites home to different sequences of Cisco Unified Communications Managers, providing load balancing across the sites.

Note The default site device pool is not created until the Type 1 to 4 site dial plan has been deployed which updates the Site Defaults to use the default device pool. If the site dial plan has not been deployed, you will not see a site default device pool in the form `Cu<customerId>Si<siteId>-DevicePool`. You can determine the default device pool for a site in Cisco Unified Communications Domain Manager 10.6(1) by selecting Site Management > Defaults.

Procedure

**Step 1** Log in as the Provider, Reseller, or Customer administrator.

**Step 2** Select the site from the hierarchy node breadcrumb at the top of the view in Cisco Unified Communications Domain Manager 10.6(1).

**Step 3** Follow the steps outlined in Create a Site Dial Plan, on page 91 if you have not already done so; the Create a Site Dial Plan, on page 91 procedure creates the default site device pool instance.

**Step 4** Log in to Cisco Unified Communications Manager and create one or more Cisco Unified Communications Manager groups on Cisco Unified Communications Manager. See Cisco Unified Communications Manager Administration Guide.

**Step 5** From Cisco Unified Communications Domain Manager 10.6(1), perform a sync operation of the Cisco Unified Communications Manager using the Administration Tools > Data Sync menu path. This sync updates the Cisco Unified Communications Domain Manager 10.6(1) cache and makes the Cisco Unified Communications Manager groups that were added directly on Cisco Unified Communications Manager available to Cisco Unified Communications Domain Manager 10.6(1).

**Step 6** Perform Associate Cisco Unified Communications Manager Group to a Device Pool, on page 171, select a Cisco Unified Communications Manager group other than the default group in the Call Manager Group drop-down list.

**Note** To verify that the phone or subscriber uses the device pool as expected, select a subscriber from the list of subscribers in Cisco Unified Communications Domain Manager 10.6(1) (Subscriber Management > Subscribers) and check the Device Pool Name setting under the Phones tab.
**Associate Cisco Unified Communications Manager Group to a Device Pool**

Use this procedure to associate a Cisco Unified Communications Manager group with an existing device pool for each site. This allows calls from a device that is tied to a device pool to go out on a specific Cisco Unified Communications Manager group based on the call type. You cannot use this procedure to add or delete device pools.

**Procedure**

**Step 1** Log in as the Provider/Reseller or Customer administrator.

When associating a Cisco Unified Communications Manager group, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to associate a Cisco Unified Communications Manager group at any other node in the hierarchy, a popup alerts you to select a site hierarchy node.

**Step 2** Perform one of the following:

- If you logged in as the Provider or Reseller Administrator, select **Device Management** > **CUCM** > **Device Pools**.
- If you logged in as the Customer Administrator, select **Device Management** > **Advanced** > **Device Pools**.

**Step 3** Click the device pool to be associated.

**Step 4** From the **Unified CM Group** pulldown menu, select a specific Cisco Unified Communications Manager group or leave the Cisco Unified Communications Manager Group as Default.

**Step 5** To save the new Cisco Unified Communications Manager group association, click **Save**.
Associate Cisco Unified Communications Manager Group to a Device Pool
Subscriber Management

- Add Subscribers, page 173
- Modify Subscribers, page 176
- Delete Subscribers, page 177
- Configure Lines, page 177
- Delete Lines, page 179
- Add Agent Line (Phone), page 179
- Configure Phones, page 180
- Delete Phones, page 183
- Quick Add Subscriber, page 183
- Voicemail, page 195
- Voicemail Workflows, page 196
- Conferencing, page 197
- Conference Workflows, page 197
- PLAR (Hotdial), page 197
- PLAR (Hotdial) Workflows, page 198
- Hunt Group Management, page 199
- Hunt Group Management Workflows, page 200
- Call Pickup Groups, page 201
- Call Pickup Groups Management, page 201

Add Subscribers

Use this procedure as a high level workflow to add one or more subscribers in Cisco Unified Communications Domain Manager.
If **Enable CSS filtering** is enabled at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under Dial Plan Management > Site > Class of Service at the particular site. If another CSS is required, you can add custom CSSs in a CSS field if you know the exact syntax.

If **Enable CSS filtering** is not enabled, then the list of available calling search spaces includes all CSSs that are configured on the Cisco Unified Communications Manager.

**Procedure**

**Step 1** Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.

**Step 2** Select a site from the hierarchy breadcrumb.

**Step 3** Go to Subscriber Management > Subscribers.

**Step 4** Click Add.

**Step 5** On the User tab, complete fields to add a Cisco Unified Communications Manager user and a Cisco Unified Communications Domain Manager user. Consider the following when adding a user:

- Use only alphanumeric characters.
- The options available in the Service Profile dropdown menu are those that were imported from Cisco Unified Communications Manager.
- If an existing phone is to be associated with a user, select the device from the Associated Devices group.
- After an existing phone is associated to the user in the Associated Devices group Device dropdown menu, click Save. The subscriber is updated so that the Phones tab is populated with the information of the new phone associated with the user.
- If the added user is configured as an LDAP user, the Password and Repeat Password fields are hidden. The Enable Mobility checkbox is auto-enabled if any of the following are included or added: a remote destination phone, mobile identity for a phone, or remote destination profile (RDP).
- Select a BLF Presence Group for the end user from the pulldown. The selected group specifies the destinations that the end user can monitor and is configured in Cisco Unified Administration. BLF Presence Group authorization works with BLF Presence Groups to allow or block presence requests between groups. The Busy Lamp Field default is set according to the selected number and specifies the Standard Presence Group that is configured with installation. For more information, see the Cisco Unified Communications Manager Features and Services Guide.

**Step 6** On the Phones tab, complete fields to add a new phone. Consider the following when adding a phone:

- Modify the values for the following fields if desired: Product Type, Device Protocol, Phone Button Template, and Device Security Profile. The possible value options for these fields change depending on which associated field is selected. For example, when you enter the Phone Name with the Product Type prefix and the MAC address, 79XX-type phones have the Phone Name “SEP” prefixed, while ATA-type phones have “ATA” prefixed to the MAC address. Fields are validated and tooltips are available to assist you to select Product Type.
• Modify phone specific settings such as DND Option dropdown menu, Do Not Disturb checkbox, and Hot Line Device. The phone settings that are available differ depending on the Product (phone) type selected, the protocol (for example SIP or SCCP), and the Field Display Policy (FDP) applied by the administrator. You can select a Mobile User ID Name from the dropdown list when a Dual Mode Phone for Android or iPhones is selected. This associates the selected user to the Mobile Identity feature on this phone and must match the Userid added on the User tab.

• The advanced settings fields are updated automatically for the phone based on the phone type. The phone is automatically associated to the user and is then displayed as an associated device when you view the subscriber after adding it. If a phone that has been associated with a user is also associated with another user, the Owner User ID defaults to the first user.

• In the Lines section of the tab, complete line assignments. Note that when you select a Route Partition Name, the available Pattern options are filtered according to the selected partition. However, you can add a custom pattern by typing it into the Pattern field. The associated Enduser field identifies the user for Presence, but you can add a new User ID. Cisco Unified Communications Domain Manager adds the user first and then adds the User ID.

• In the Speeddial section, add speed dial information. Available speed dials depend on the Phone Button Template.

• In the Blf Directed Call Park section, specify Busy Lamp Field Directed Call Park values. Values depend on a valid Directed Call Park on Cisco Unified Communications Manager.

• In the Add On Module section, specify Add On Modules if desired. The Add On Modules Load Name can be any value, but the Model has to be supported by the phone.

• In the Service section, add services that are valid IP services for Phones. To add a service to the device, a number must be added as the Uri Button index. If you do not add a number, only the service is added.

• Use the Mobile Identity form to configure mobile identity details when you select a Dual Mode Phone. Fields include: Name, Dual Mode Device Name (automatically populated from the Device Name field), and Mobility Profile Name (chosen from a dropdown list). The Destination field is a mandatory field and determines the destination number that is dialed when a call is made to the dual mode phone.

• Use the Remote Destination Phone form to configure your remote destinations when a Dual Mode Phone is selected. Remote destinations represent the mobile (or other) phones that are able to accept transfer from the desktop phone and can be used to initiate calls. Set the Pattern for the Line Association to the Route Partition name. If you enter more than one Pattern and the new Pattern is not on the system, enter the Route Partition Name manually.

• Use the Vendor Config section of the tab to view and edit the configuration settings for each device. The available configuration settings depend on the each Product type selected. Modify settings as required.

**Step 7** On the Extension Mobility tab, complete fields to configure Extension Mobility for the end user. Consider the following:

• Only one Device Profile can be added for extension mobility.

• As with the Phones tab, Product Type, Device Protocol and Phone Button Template fields change, depending on the selection of an associated field.

• The fields on this tab behave in the same way that they do on the Phones tab, with the exception of Remote Destination information, which is not available on Device Profiles.
• Ensure that you associate the Extension Mobility Device Profile and target phone for login with the Extension Mobility service.

**Step 8** On the **Single Number Reach** tab, note that you cannot add more than one Remote Destination Profile for Single Number Reach. However, you can add more than one Remote Destination Rdp.

**Step 9** On the **Voicemail** tab, configure voice mail service for the end user if a valid Cisco Unity Connection server is available. Consider the following when configuring voice mail:

• You can leave the PIN and Password empty, in which case the default credential policy on the Cisco Unity Connection is used.

• If a user is prompted from ImportUsers to an LDAP Cisco Unity Connection user, the Password field is visible but should not be ignored. This is because there is no way to know that the user being added is an LDAP-synced user.

• The Voicemail Line dropdown list shows available lines but you can also add values manually. The Cisco Unity Connection server uses this line as a caller ID, so you should set it to the user's default line.

**Step 10** On the **WebEx** tab, add details if a valid server is available. The mandatory fields on this tab are populated with the values entered on the **User** tab. Note however, that any updates on the **User** tab do not update these values; values are populated only during the Add workflow.

**Step 11** When you are finished adding information for the subscriber, click **Save**.

**Step 12** Repeat steps 4 to 11 to add another subscriber.

## Modify Subscribers

Use this procedure to modify settings for one or more subscribers.

**Procedure**

**Step 1** Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.

**Step 2** Select a site from the hierarchy breadcrumb.

**Step 3** Go to **Subscriber Management > Subscribers**.

**Step 4** Choose the subscriber to be updated by clicking on its box in the leftmost column, then click **Edit**.

**Step 5** Modify subscriber information as required, using the workflow described in [Add Subscribers](#), on page 173. **Note** If more than one Phone is added, you can use the pop-up form that is available when modifying the Subscriber on the Phones tab. Alternatively, for one-to-many or zero-to-many item instances such as a Phone, it can be deleted.

**Step 6** Click **Save**.
Delete Subscribers

Use this procedure to delete one or more subscribers.

Procedure

Step 1 Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.

Step 2 Select a site from the hierarchy breadcrumb.

Step 3 Go to Subscriber Management > Subscribers.

Step 4 Choose the subscriber to be deleted by clicking on its box in the leftmost column, then click Delete.

Step 5 From the popup window, click Yes to confirm the deletion.

Note For scenarios that include an LDAP-integrated Cisco Unified Communications Manager, the process for deleting a user is from the LDAP directory and not from the Cisco Unified communications Domain Manager system. Set up a data sync to synchronize the removal of the user.

When the delete action is complete, the Subscriber disappears from the list. All elements associated with the Subscriber are deleted, except Lines.

Configure Lines

Use this procedure as a high level workflow to configure one or more lines (directory numbers) in Cisco Unified Communications Domain Manager. Note that if the Number Inventory feature has been enabled by the administrator, lines are not added; rather, lines are selected from a dropdown list of available numbers.

Note The Lines interface in Cisco Unified Communications Domain Manager provides an easy method to add, modify, or delete individual lines and associated line settings to, or from the system. For inbound calls to work from PSTN, make sure that the line has the correct E.164 alternate number configured.

Procedure

Step 1 Log in as a provider, customer, or site level administrator. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.

Step 2 Select a site from the hierarchy breadcrumb.

Step 3 Go to Subscriber Management > Lines.

Step 4 Click Add.

Step 5 Configure the line and its associated line settings using the following tabs. For more information on the values to fill in for the various line parameters such as partitions and CSS, refer to the Cisco Hosted Collaboration Solution, Release 10.6(1) Dial Plan Management Guide for Cisco Unified Communications Domain Manager, Release 10.6(1).
If **Enable CSS filtering** is enabled at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under **Dial Plan Management > Site > Class of Service** at the particular site. If another CSS is required, you can add custom CSSs in a CSS field if you know the exact syntax.

If **Enable CSS filtering** is not enabled, then the list of available calling search spaces includes all CSSs that are configured on the Cisco Unified Communications Manager.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number Basic Information</td>
<td>Includes a directory number (mandatory), a route partition, calling search space, call pickup group (to which the line belongs), and other basic settings. The Directory Number field is either a dropdown list or a free text field, or a dropdown containing only the available directory numbers (depending on whether the Number Inventory feature is enabled or disabled). Only the actual Directory Number is mandatory.</td>
</tr>
<tr>
<td>Directory Number Advanced Information</td>
<td>Includes various profiles, groups, and advanced settings for the line; for example, voice mail profiles. It also includes enterprise and E.164 alternate number information, as well as URIs.</td>
</tr>
<tr>
<td>Shared Device Info</td>
<td>Shows any phones, device profiles, or remote destination profiles that have been associated with the particular line.</td>
</tr>
<tr>
<td>Line Settings for all Devices</td>
<td>Includes fields such as hold reversion ring duration, hold reversion notification interval, party entrance tone (selected from a dropdown list).</td>
</tr>
<tr>
<td>AAR Settings</td>
<td>Automated alternate routing (AAR) handles the calls that are routed to the AAR Destination Mask or Voice Mail.</td>
</tr>
<tr>
<td>Park Monitoring</td>
<td>Includes text fields such as park monitoring forward no retrieve destination external or internal voice mail enabled check boxes, park monitoring forward no retrieve destination external, external calling search space, internal, internal calling search space, and park monitoring reversion timer text fields.</td>
</tr>
<tr>
<td>Call Forwarded Information</td>
<td>Includes call forward all settings, call forward busy external and internal settings, call forward no answer external and internal settings, and so on.</td>
</tr>
</tbody>
</table>

**Note** If **Enable CSS filtering** is enabled at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under **Dial Plan Management > Site > Class of Service** at the particular site.

If **Enable CSS filtering** is not enabled, then the list of available calling search spaces includes all CSSs that are configured on the Cisco Unified Communications Manager.

**Step 6** When you are finished adding line information, click **Save**.
All additions or changes to Lines and line settings in the system are also reflected in the Cisco Unified Communications Manager. After configuring a line, the transaction menu item (Administration Tools > Transaction) can be used to verify the configuration.

**Step 7** To modify existing line and line setting details, change the settings or add new line settings using the process described in Steps 1 to 6. For example, you can add additional directory URIs and directory URI partitions. Manual configuration must first be done on the Cisco Unified Communications Manager before URs will function. Note that not all line settings are configured using Subscriber Management > Lines. Device specific settings such as caller ID display, line label, E.164 mask, and associated user are configured with the Phones and Subscriber menu items.

---

## Delete Lines

Use this procedure to delete one or more lines, or line settings.

**Procedure**

**Step 1** Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site you can see all the fields described in this procedure. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.

**Step 2** Select a site from the hierarchy breadcrumb.

**Step 3** Go to Subscriber Management > Lines.

**Step 4** Choose one of the following methods to delete lines or line settings:

- Choose an individual line to be deleted by clicking on its box in the leftmost column, then click Delete. From the popup window, click Yes to confirm the deleted line.
- Delete multiple lines at once by checking the relevant check boxes, then clicking Delete. From the popup window click Yes to confirm the deleted lines.
- Remove line settings from a line as required by removing them from the relevant tab of a selected line. Click Save.

When the delete action is complete, the line disappears from the list.

---

## Add Agent Line (Phone)

**Procedure**

**Step 1** Navigate to Subscriber Management > Agent Lines.

**Step 2** On the Agent Lines page, click the Add icon to add a new agent line

**Step 3** Do the following:
Select the device type: Phone Device Type
Select the name of the Cisco Unified Communications Manager Phone. This is a mandatory field. Device Name
Select the line to be marked as an agent line. This is a mandatory field. Line
Select the application user to be associated with the Phone. This is a mandatory field. Application User
CC_Line. This is read only. Agent Line Prefix

**Step 4**  Click the Create icon to add the agent line.

## Configure Phones

Use this procedure as a high level workflow to configure one or more phones and associated settings. Note that if the Number Inventory feature has been enabled, phone lines are not added; rather, phones are selected from a dropdown list of available numbers.

The Phones menu screen is an integrated display to add, modify, or delete the following on the Cisco Unified Communications Manager device:

- A Line. If the line does not exist, it is created.
- Devices and device details related to the user
- The association of a line with the user's device
- For a Dual Mode Phone, if a mobile identity is provisioned, it is added to the phone. Additional remote destinations can be added if desired.
- The User is updated. Note that for a Dual Mode Phone, the Mobility User ID Name must be set.

When adding a device for a subscriber, ensure that the following properties of the selected device are related correctly:

- Product
- Protocol
- Security Profile Name
- Phone Template Name. If a new phone is added to Cisco Unified Communications Manager using COP files, the phone and associated template are only available in Cisco Unified Communications Domain Manager after it has been synced with Cisco Unified Communications Manager.
Before You Begin

To ensure that the Add Phones workflows execute successfully, create and configure the following items first on Cisco Unified Communications Manager and then import them into the Cisco Unified Communications Domain Manager:

- Softkey templates and phone button templates
- Service parameters and enterprise parameters that must be set for a subscriber service
- Custom SIP profiles
- Service profiles for Jabber
- Phone services

During the end-to-end creation of providers, customers, and sites, default values are created (for example, Site ID), and if the dial plan for the site specifies Device Pool, CSS, and Partition names, these are available for selection. To identify these site-related values, refer to the naming conventions used in the “Modify Site Defaults” procedure in this guide.

Certain default values for phones are populated by the Site Defaults Menu item which can be viewed and edited (depending on your login level). Go to Site Management > Defaults and click on the required site name in the list view. For phone parameter information, fields can be found in the General Defaults and Device Defaults tabs. Refer to the "Modify Site Defaults" procedure in this guide for additional information regarding the values to fill in for phone parameters such as partitions and CSSs.

Note

If Enable CSS filtering is enabled at the customer dial plan, then for all calling search space fields in this procedure, the list of available calling search spaces includes only those that are marked as a Class of Service under Dial Plan Management > Site > Class of Service at the particular site. If another CSS is required, you can add custom CSSs in a CSS field if you know the exact syntax.

If Enable CSS filtering is not enabled, then the list of available calling search spaces includes all CSSs that are configured on the Cisco Unified Communications Manager.

Procedure

Step 1 Log in as a provider, customer, or site level administrator. If you are logged in as the site administrator, you can see a subset of the fields that are available on the interface.

Step 2 Select a site from the hierarchy breadcrumb.

Step 3 Go to Subscriber Management > Phones.

Step 4 Click Add.

Step 5 Configure the phone and its associated settings using the following tabs.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>Default values for Protocol and Phone Template name fields are updated automatically based on the selected product type.</td>
</tr>
</tbody>
</table>
The Vendor Config area displays the configurable vendor features available for the selected phone type. Configure each field as required. Note that the fields displayed are different, depending on the selected product (device type), as well as the device protocol; for example, SIP or SCCP. The availability of the Vendor Config settings depends on the Field Display Policy.

### Advanced Information
This tab serves two purposes:

1. To show all the lines that are associated with the device
2. To associate lines with the device.

The Lines sections reflect the Lines object in Cisco Unified Communications Manager. You can add lines to this group and associate lines with the device. You can add custom lines by entering a line instead of selecting an existing line from the dropdown list (depending on the status of the Number Inventory feature).

### Lines
Allows you to configure speed dials for the device. Available speed dials depend on the device’s Phone Button Template. The order in which Speed Dial entries are added matches the slots that are available in Cisco Unified Communications Manager.

### Speed Dials
Used to set IP Phone services.

### Busy Lamp Fields
Allows you to configure busy lamps for the device. Available busy lamp fields depend on the device's Phone Button Template.

### BLF Directed Call Parks
Allows you to configure BLF directed call parks for the device. Available BLF directed call parks depend on the device's Phone Button Template. BLF directed call parks must first be created in Call Routing > Directed Call Parks on the Cisco Unified Communications Manager before they can be configured for a device from this tab. The available BLF directed call parks match those created for each specific Route Partition Name.

### Dual Mode Settings
Only applies to Dual Mode phones, and allows you to enter the relevant Mobile Identity and Remote Destination parameters for the Dual Mode phone. These include: Name, Destination, Dual Mode Device Name of the Phone, Answer Too Soon and Too Late Timers, and so on.

### Step 6
When you are finished adding phones and phone settings, click **Save**.

### Step 7
To modify existing phone and phone settings, change the settings or add new phone settings using the process described in Steps 1 to 6. When you modify a phone, the following workflow is executed (depending on what was modified):

- When adding a line, a check is made to see if it exists. If the line does not exist, it is created.
- The Phone and User Remote Destination are updated.
Delete Phones

Use this procedure to delete one or more phones, or phone settings. When phones are deleted, the following occurs:

- The Remote Destination is removed first, so that the Cisco Unified Communications Domain Manager cache remains in sync with the Cisco Unified Communications Manager.
- The Phone is deleted.

Note: Lines are not affected.

Procedure

Step 1 Log in as a customer or site level administrator. If you are logged on as the customer administrator for a specific site, you can see all the fields described in this procedure. If you are logged on as the site administrator, you can see a subset of the fields that are available on the interface.

Step 2 Select a site from the hierarchy breadcrumb.

Step 3 Go to Subscriber Management > Phones.

Step 4 Choose one of the following methods to delete phones or phone settings:

- Choose an individual phone to be deleted by clicking on its box in the far left column, then click Delete. From the popup window, click Yes to confirm the deleted phone.

- Delete multiple phones at once by checking the relevant check boxes, then clicking Delete. From the popup window, click Yes to confirm the deleted phones.

- Remove phone settings as required by removing them from the relevant tab of a selected phone. Click Save.

When the delete action is complete, the phone disappears from the list.

Quick Add Subscriber

The purpose of the Quick Add Subscriber interface is to provide a single input form to add users on Unified Communications Manager as well as selected Voicemail and WebEx accounts, and to provide them with services such as SNR, Extension Mobility, and Jabber Device (Mobile Identity).

The Quick Add Group, which is a conglomeration of individual templates that configure each of the subscriber features, is required.

The interface also makes it possible to add lines for the Unified CM user.
In order to add subscribers using Quick Add Subscriber, a default user template "voicemailtemplate" must already exist on the Unified CM. It is possible, as a part of Dial Plan management, to change this default by editing the Default CUC User Template value in the Site Defaults reference.

In order for self-provisioned phones to show as associated with a Subscriber, administrators should carry out a Cisco Unified Communications Manager Data Sync after setting up a self-provisioned phone.

Any modification of the added subscriber and associated services are done from the respective service menu item.

**Configuration**

In order to create or provision any users, enable them with services or associate them with devices, certain configurations must be done on the system.

**Server Configurations**

The following servers need to be configured in Cisco Unified Communications Domain Manager:

1. Cisco Unified Communications Manager Server - Adding a Cisco Unified Communications Manager server is a required configuration. It is required to:
   1. Sync manually provisioned users or LDAP Integrated users in Cisco Unified Communications Manager to Cisco Unified Communications Domain Manager.
   2. Sync any of these users existing associated Phones, Directory Numbers, Extension Mobility Profiles in Cisco Unified Communications Manager to Cisco Unified Communications Domain Manager.
   3. Create Subscribers (push users to Cisco Unified Communications Manager).
   4. Push user's associated Phones, Directory Numbers, Extension Mobility Profiles, etc to Cisco Unified Communications Manager if any exist.

2. LDAP Server - in order to provision LDAP Synced users in Cisco Unified Communications Domain Manager, an LDAP Server will be required. Otherwise it will be an optional step.

3. Cisco Unity Connection Server - A Cisco Unity Connection Server is required only to add any Cisco Unity Connection voicemail users that are configured in Cisco Unified Communications Domain Manager.

**DialPlan Deployment**

A DialPlan needs to be configured at both the Customer and Site hierarchies where the users will be provisioned.

**Voicemail Service**

A Voicemail Service has to be deployed with a pilot number created and associated to a site under Services > Voicemail in Cisco Unified Communications Domain Manager in order to create a "Default CUC Subscriber Template" under Site Defaults > CUC Defaults. This template is required for creating any CUC Voicemail users.

**Webex Service**

The WebEx Server needs to be configured in Cisco Unified Communications Domain Manager to be able to deploy any Webex users provisioned through QAS. A password for the Webex users needs to be defined in Site Defaults.
Quick Add Subscriber Conditions

In order to create users using Quick Add Subscriber, certain conditions must be followed:

1. From the Quick Add Subscriber Group menu, create a custom group or continue using the default group.

2. Existing Users can be provisioned in Cisco Unified Communications Manager through Quick Add Subscriber only if they exist at the Site level.

3. LDAP synced or LDAP Integrated at Cisco Unified Communications Manager user fields are always read only and cannot be edited.

4. A Line can be associated to Multiple phones.

5. A Phone can be associated to multiple lines.

6. Since multiple voice accounts can be created for a user the voice checkbox is always visible on the gui.

7. There can only be one extension mobility profile per user.
   - The Extension Mobility checkbox will not be visible once an EM Profile is created.

8. There can only be one Webex account per user.

9. Multiple Jabber Devices can be associated to a user. They don't have any line associations.

10. There can only be one self service id per user. This is set from the Self Service ID checkbox and can always be updated by assigning a new line from QAS in Cisco Unified Communications Domain Manager.

11. DN is created in Cisco Unity Call Manager in two ways:
    - By creating a voicemail line in QAS.
    - By creating just a Line in QAS.

   Whenever a voicemail or voicemail line is created using Quick Add Subscriber, the DN "used" field is set to true under Subscriber Management > Directory Number Inventory.

12. DN created without any device associations (voicemail line) is tagged under Subscriber Management> Lines as "DN created without device from QAS".
Workflows

Workflow for Creating Configuration Templates

Procedure

Step 1  Login as HcsAdmin or Provider Admin.

Step 2  Go to Role Management > Configuration Templates.

Step 3  Open a configuration template from the existing ones whose properties are to be cloned for the custom one. Select Action > Clone on the top right of the screen.

Step 4  Edit the cloned template fields before saving as per the requirement.

Note: Certain dropdown fields only populate choices depending on specific conditions. Please refer to CSCur61890 release notes.

Example: To create a template for the Cisco 6941 SCCP Phone:

a) Set into the hierarchy where the Cisco Unified Communications Manager to be used exists. This step is required if the dropdown fields have to populate values because some of the values are derived from the actual device model through API.

b) Clone the "Default CUCM Phone Template". Do not save yet.

c) Change the template name and description.

d) Select "SCCP" from the Protocol field dropdown.

e) Select "Standard 6941 SCCP" from the Phone Template Name field dropdown.

f) Select the "Cisco 6941 - Standard SCCP Non-Secure Profile" from the Security Profile Name field dropdown.

g) Select the "Cisco 6941" from the Product field dropdown.

h) Select the "Standard Presence Group" from the Presence Group Name field dropdown.

i) The rest of other fields can use the default cloned values.

Note: The above step values can also be manually inputted instead of selecting from dropdowns if the values are known to the admin.

Step 5  Click on Save.

The template would get created at the hierarchy level you used.
Workflow for creating Quick Add Subscriber Groups

Procedure

Step 1 Log in as an Admin (Provider, Reseller, Customer or Site).
Step 2 Go to Subscriber Management > Quick Add Subscriber Groups.
Step 3 Click on Add.
Step 4 Enter the Group Name. This is a required field.
Step 5 Select the appropriate template from the dropdowns for the template field you choose to use.
   Example To create back office QAS users with phone type 6911 using SCCP protocol (voice account):
   a) Select the "Backoffice Phone 6911 SCCP" template from the dropdown in the GUI for the Default CUCM Phone Template field.
   b) Select the "Default CUCM Line Template" for the Default CUCM Line Template field in order to associate a line with the phone.
   c) Custom configuration templates described above can also be used to assign to a Quick Add Subscriber Group.
      Note: The custom configuration template has to be at the same hierarchy the group is at.
Step 6 Click on Save.

Workflow for Creating Subscribers

Existing Users
Existing Users already exist at the Site level under User Management > Users but are not yet pushed to the Cisco Unified Communications Manager.

1 Create a custom Quick Add Group or use the default Quick Add Group
2 Go to Subscriber Management > Quick Add Subscribers.
3 Select the user from the "Username" drop down.
4 The user data fields like First Name, Last Name are populated with values that exist for that user under User Management > Users.
5 Select the Quick Add Group to be assigned to the user
   • It is defaulted to "default" value.
6 Edit the user fields if required. Provision new services to the user if required as described in the workflow below.
7 Click Save.

New Users
These users do not yet exist in Cisco Unified Communications Domain Manager and Cisco Unified Communications Manager.
1. Go to **Subscriber Management > Quick Add Subscribers**.
2. Input the username in the "Username" drop down.
3. Input the mandatory Last Name field.
   - `FirstName` is optional but required for configuring a Webex account.
4. Select the Quick Add Group to be assigned to the user.
   - It defaults to the "default" value.
5. Provision new services to the user if required as described in the workflow below.
6. Click **Save**.

**Workflow for Updating Subscribers**

These are the users that already exist under **User Management > Users** and also in Cisco Unified Communications Manager.

**Procedure**

**Step 1** Go to **Subscriber Management > Quick Add Subscribers**.
**Step 2** Select the subscriber to be updated from the **Username** drop down.
**Step 3** The user data fields like `FirstName`, `LastName` are populated with values that exist for that user under **User Management > Users**. Any associated devices or subscribed services for the user will show up under the **Existing Services** tab.
**Step 4** Select the **Quick Add Group** to be assigned to the user.
   - It is defaulted to **default** value.
**Step 5** Edit the user fields if required. Provision new services to the user if required described in the workflow below.
   - The Quick Add Subscriber conditions described earlier will be complied while provisioning any existing services.
**Step 6** Click **Save**.

**Workflow for Provisioning Services to Users**

**Voice**

1. Go to **Subscriber Management > Quick Add Subscribers**.
   - Select the user from the **Username** drop down.
2. Create a "Voice" device for the User.
   - Select the **Voice** check box.
   - The **Lines** and **Phones** fields are highlighted in red.
• Click on + in the Lines field.
• The Directory Number drop down field is displayed.
• Select a Line from the drop down.
  • The Line must have be a Directory Number under Subscriber Management > Directory Number Inventory.
• Click on + in the Phones field.
• The Phone Name field is displayed.
• Input a valid Phone Name in the Phone field. eg: SEP00000005001
  • Multiple Phone Devices can be added using +.
• Click Save.

3 Verify the voice device got associated to the Subscriber.
  • Go to Subscriber Management > Quick Add Subscribers.
    • Select the above user from the Username drop down.
    • Select the Existing Services Tab.
    • The Phones field will display all the Phone devices information along with their line associations.

Extension Mobility

1 Go to Subscriber Management > Quick Add Subscribers.
  • Select the user from the Username drop down.

2 Create an "Extension Mobility Profile".
  • Select the Extension Mobility checkbox.
  • Click Save.

3 Verify the Extension Mobility profile got created for the Subscriber.
  • Go to Subscriber Management > Quick Add Subscribers.
    • Select the above user from the Username drop down.
    • Select the Existing Services Tab.
    • The Extension Mobility field will display the Extension Mobility profile name.

Voicemail

1 Go to Subscriber Management > Quick Add Subscribers.
  • Select the user from the Username drop down.
2 Create a "Voicemail" line.
   • Select the Voicemail checkbox.
   • The Line field is highlighted in red.
   • Click on + to add a Line.
   • The Directory Number drop down field is displayed.
   • Select a Line from the drop down.
   • Click Save.

3 Verify the Voicemail line got created for the Subscriber.
   • Go to Subscriber management > Quick Add Subscribers.
     • Select the above user from the Username drop down.
   • Select the Existing Services tab.
   • The Voicemail field will display the voicemail line.

Webex
1 Go to Subscriber Management > Quick Add Subscribers.
   • Select the user from the Username drop down.

2 Create a Webex account.
   • Select the Webex checkbox.
     • First Name is required for activating a Webex account.
     • If the First Name doesn't exist, the First Name field is highlighted in red.
     • Input the First Name if it doesn't exist.
   • Click Save.

3 Verify the Webex account was created for the Subscriber.
   • Go to Subscriber Management > Quick Add Subscribers.
     • Select the above user from the Username drop down.
   • Select the Existing Services tab.
   • The Webex field will display ACTIVATED.

Single Number Reach
1 Go to Subscriber Management > Quick Add Subscribers.
   • Select the user from the Username drop down.
2 Create a **Single Number Reach** profile.

- Select the **Single Number Reach** checkbox.
- The **Mobile Number** field is displayed.
  - Input the Mobile Number in the right format without any spaces and special characters.
  - The Mobile Number can be the same as the Mobile Number (if it exists) for this user (unless the user is new) under **User Management > Users**.
- Click **Save**.

3 Verify the Single Number Reach profile was created for the Subscriber.

- Go to **Subscriber Management > Quick Add Subscribers**.
  - Select the above user from the **Username** drop down.
  
  - Select the **Existing Services** tab.
  
  - The **Single Number Reach** field will display the actual profile name.
    - The profile name is a combination of username and the text "RDP" cojoined by ".-". For example, user5001-RDP.

**Jabber Device**

1 Go to **Subscriber Management > Quick Add Subscribers**.

- Select the user from the **Username** drop down.

2 Create a Jabber Device.

- Select the **Jabber Device** checkbox.
- The Jabber Devices column is displayed.
- Click on the + which displays the following fields:
  - Jabber Agent
  - Device Name

- Select a device type from the **Jabber Agent** drop down.
- Input the Device Name in the right format.
- Below are the device type and device name combinations.

<table>
<thead>
<tr>
<th>Device</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Bot&lt;&lt;Name&gt;&gt;</td>
</tr>
<tr>
<td></td>
<td>BOT123</td>
</tr>
<tr>
<td>CSF</td>
<td>&lt;&lt;Name&gt;&gt;</td>
</tr>
<tr>
<td></td>
<td>123</td>
</tr>
</tbody>
</table>
3 Verify the Jabber Device account was created for the Subscriber.
   • Go to **Subscriber Management > Quick Add Subscribers**.
     • Select the above user from the **Username** drop down.
     • Select the **Existing Services** tab.
     • The Phones field will display the Jabber Device.

**Self Service Id**

1 Go to **Subscriber Management > Quick Add Subscribers**.
   • Select the user from the **Username** drop down.

2 Create a Self Service Id for Self Provisioning.
   • Select the **Self Service Id** checkbox.
   • The Line field is highlighted in red.
   • Click on + to add a Line.
   • The **Directory Number** drop down field is displayed.
   • Select a Line from the drop down.
   • Click **Save**.

3 Verify the Self Service Id line was created for the Subscriber.
   • Go to **Subscriber Management > Subscribers**.
     • Select and open the above user.
     • The **Self Service** field displays the Id created.
       • It's usually synonymous with the line when created through Cisco Unified Communications Domain Manager.
       • It creates a primary extension in Cisco Unified Communications Manager for that user which consists of a Pattern and a Route Partition Name.
Workflow for Deleting Subscribers

Delete Subscriber

Subscribers can be deleted/unprovisioned from the system in the following ways:

1. Delete the Subscriber from **Subscriber Management > Subscribers**.
2. Remove Users from CUCM action from **User Management > Manage Users**.

Deleting a Subscriber is the recommended method rather than using the "Remove User from Cisco Unified Communications Manager" option.

The delete workflow pattern differs for scenarios defined by the following two constraints:

- Subscriber Type: Ldap or Non Ldap users
- Device Associations

The Subscribers can be broadly categorized into the following users:

- **Non LDAP Synced Users**: All the following users come under this category
  - users created in Cisco Unified Communications Domain Manager 10.6(1) and pushed to Cisco Unified Communications Manager.
  - users provisioned in Cisco Unified Communications Manager and synced to Cisco Unified Communications Domain Manager 10.6(1).

- **LDAP Integrated at Cisco Unified Communications Domain Manager 10.6(1) Users**: These users are LDAP integrated at Cisco Unified Communications Manager and are synced to Cisco Unified Communications Domain Manager 10.6(1).

- **LDAP Synced Users**: All these users are directly synced from an LDAP Server to Cisco Unified Communications Domain Manager 10.6(1).

The Subscribers can either have

- Associated devices like Phones, Extension Mobility, Single Number Reach, Voicemail and Webex.
- No Associations.

Delete Subscriber

Below is a detailed description of how to delete/unprovision Subscribers.

1. From the left menu, go to **Subscriber Management > Subscribers**.
2. Select the Subscriber you want to remove.
3. Click **Delete**.

**Non LDAP Synced Users / LDAP Integrated at Cisco Unified Communication Manager Users**

- **With Devices**
  - Deletes all devices.
Remove Users from Cisco Unified Communications Manager

Below is a detailed description of how to remove Users from Cisco Unified Communications Manager.

1. From the left menu, go to **User Management > Manage Users**.
2. Select the **Remove Users from CUCM** action.

**Non LDAP Synced Users / LDAP Integrated at Cisco Unified Communication Manager Users**

• With Devices
• Doesn't delete the user from Cisco Unified Communications Manager
• Doesn't delete any of the below associations for the user from Cisco Unified Communications Manager.
  ◦ Phones : device/cucdm/Phone
  ◦ Single Number Reach : device/cucm/RemoteDestinationProfile
  ◦ Extension Mobility : device/cucdm/DeviceProfile
  ◦ Voicemail : device/cuc/User
  ◦ WebEx : device/webex/User

• A log message is generated under User Management > Log Messages that contains the details of why the user was not deleted and a list of associated devices for that user.

• Without Devices
  • Removes the user from the Cisco Unified Communications Manager. (device/cucm/User)
  • Removes the Cisco Unified Communications Manager Server from the Provisioning Status.

LDAP Synced users
• With Devices
  • Doesn't delete the user from Cisco Unified Communications Manager.
  • Doesn't delete any of the below associations for the user from Cisco Unified Communications Manager.
    ◦ Phones : device/cucdm/Phone
    ◦ Single Number Reach : device/cucm/RemoteDestinationProfile
    ◦ Extension Mobility : device/cucdm/DeviceProfile
    ◦ Voicemail : device/cuc/User
    ◦ WebEx : device/webex/User

  • A log message is generated under User Management > Log Messages that contains the details of why the user was not deleted and a list of associated devices for that user.

• Without Devices
  • Removes the user from the Cisco Unified Communications Manager. (device/cucm/User)
  • Removes the Cisco Unified Communications Manager Server from the Provisioning Status.

Voicemail

The Voicemail interface makes it easy for an Administrator to add, modify or delete CUC Voicemail users as well as associated Voicemail services from a single tabbed form. The user that is added to the system is
also added to the CUC Voicemail system, and if the relevant services are selected these are also added to the CUC Voicemail system.

The following can be provisioned by means of the Voicemail interface:

- **CUC Account** - A CUC User, which includes a VM account name, a VM number and an associated subscriber template. The CUC Subscriber Template default value is pulled from the Site Defaults menu, which can be viewed and edited (if logged in at the appropriate administrator level) by choosing the CUC Defaults tab from **Dial Plan Management > Site Defaults**.

- **Alternate Extensions** - Alternate extension numbers that are available to the CUC Voicemail user.

- **Credentials** - Password and PIN

- **Notification Devices** - Devices used to notify the CUC user of Voicemails sent to the user. These include: Phone, HTML, SMTP (email), Pager, and SMS (if an SMPP Provider has been added on the relevant Voicemail server)

### Voicemail Workflows

A Voicemail account can only be added if:

- The administrator has navigated to the relevant Provider, Customer, Site level.

- A CUC Server (VM Server) has already been provisioned at the Global, Provider, or Customer level.

- A Network Device List (NDL) and NDLR points have already been created.

When adding a new Voicemail account, the following workflow is executed:

1. A CUC account is added with the details input by the user.
2. Alternate extensions are added with the details input by the user (if applicable).
3. Credentials (password and PIN) are added with the details input by the user. The password and PIN can either be locked by the administrator, or the user can be prompted to change the credentials upon first login.
4. Notification Devices are added. The system automatically provisions default notification devices, however additional notification devices can also be added when adding a Voicemail account.

You can modify either an existing Voicemail account service information (details that were added to a Voicemail account during the Add Voicemail process), or you can modify a Voicemail account by adding new Voicemail services (those that were not added to the Voicemail account during the initial Add Voicemail process). For example, you can add additional alternate extensions and/or notification devices. After adding a Voicemail service to a subscriber, any lines that are used by any of the devices associated to the subscriber must be updated to reflect the proper call forward and Voicemail profile settings to enable the Call Forwarding to Voicemail and Voicemail buttons.

When modifying a Voicemail account, the workflow and processes are executed as with the Add workflow.

- Modular Add and Delete workflows can be carried out. For example, if more than one alternate extension or notification device is added to the Voicemail account, a pop-up form is available on the appropriate Alternate Extensions tab or Notification devices tab. Alternatively, for one-to-many or zero-to-many item instances such as an alternate extension, it can be deleted. These Add and Delete operations carry out a secondary workflow on the Voicemail instance.
When deleting a Voicemail account, the following should be noted about the workflow:

1. All elements associated with the Voicemail account are deleted.
2. Modular Delete workflows can be carried out as a part of a Modify workflow.

**Conferencing**

Site administrators manage the conferencing credentials of users if a WebEx server is available at the site level. The WebEx server on which users are administered can be identified with the Network Device Reference of the site, or else (according to the common reference resolution process) with the first such server in the current or higher up hierarchy level.

The default Conferencing input form that provides the interface to WebEx users displays the minimum of WebEx user properties that are mandatory. The Field Display Policies and Configuration Templates for this Conferencing input form can be modified according to the suggested customization procedure for Policies and Templates.

If conferencing was added for a Subscriber user when the Subscriber was added, the WebExId is defaulted to the userid. Note that the WebEx user properties that are shown on the Subscriber form may not correspond with those shown on the Conferencing input form. If the Conferencing feature is to be added for an existing subscriber, make sure that the WebExId is the same as the userid.

For Conference Workflows to function, make sure that the following is done at the Customer:

- A WebEx server is added.
- The WebEx server is added to a Network Device List (NDL).
- The required site references the relevant NDL.

**Conference Workflows**

User details can be added if a valid server is available.

When adding Conferencing from this input form, the mandatory fields are entered on the WebEx server. Conferencing details can also be added as part of Subscriber Management. If the WebEx Id is a Cisco Unified Communications Domain Manager 10.6(1) and Unified CM username of a Subscriber, the WebEx details are displayed on its Subscriber Management screen WebEx tab.

Modify Conferencing details on the selected item, or also add and delete details from the Subscriber Management form.

Deleting a Conference item will remove the details from the WebEx tab of Subscriber Management if the user is a Subscriber.

**PLAR (Hotdial)**

The Private Line Automatic Ringdown (PLAR) feature, also called Hotdial, automates the Unified CM configuration required to set up PLAR for a phone. The PLAR feature provides an administrator with a single interface and workflow for the management of the following elements of Unified CM:
• RoutePartition
• CSS
• TransPattern
• Phone
• Line
• SIP Dial Rule

The feature further provides an administrator with:
• A simplified user interface to select a Phone that must be enabled for PLAR, a destination number, and the destination CSS.
• The orchestration of a workflow to create the necessary Unified CM partition, CSS, Translation Pattern, and so on, and to apply these to the relevant Phone and Number.

To configure an existing phone for Hotdial, the user selects a pre-existing device and indicates that the device is a Hotdial device.

As soon as a PLAR configured phone goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a pre-configured destination number. The phone cannot dial any other number except the Hotdial destination that gets configured for PLAR.

The PLAR configuration can be added or deleted, but not modified.

**PLAR (Hotdial) Workflows**

When adding a new Hotdial Phone (PLAR configuration), the following workflow is executed:

1. A Unified CM route partition is created with:
   a. Name set to the selected Hotdial destination prefixed with "HotdialPT-".
   b. Description set to the Hotdial destination prefixed with "Hotdial Partition for Destination".
   c. Time Zone set to the time zone defined for the site.
   d. Partition Usage is set to General.

2. A Unified CM CSS is created with:
   a. Name set to the selected Hotdial destination prefixed with "HotdialCSS-".
   b. Description where the selected Hotdial destination is prefixed with "CSS for Hotdial/PLAR Destination".
   c. The Partition created above is made a member of the CSS.
   d. Partition Usage is set to General.

3. A Unified CM translation pattern is created with:
   a. Route Partition Name is set to the selected Hotdial destination prefixed with "HotdialPT-".
   b. Description is set to the selected Hotdial destination prefixed with "Used in Hotdial/PLAR for Destination".
c Calling Search Space Name set to the selected destination dialing CSS.
d Called Party Transformation Mask is set to the selected Hotdial destination.
e Route Option is set to Route this pattern.
f For SIP Phones only, a SIP Dial rule is created and the phone is set to use the SIP Dial Rule.

4 The Unified CM phone selected is updated as follows:
a CSS name set to the selected Hotdial destination prefixed with "HotdialCSS-".
b Hotline Device is set to true if the phone is marked as a Hotline Device by the user on the input form.

5 The Unified CM directory number selected as the Hotdial destination is updated as follows:
a The Route Partition Name is set to the route partition added in Step 1 above.

Cisco Unified Communications Domain Manager 10.6(1) automatically resets the phone when required.

When deleting Hotdial to disable Hotdial for a Phone (deleting the PLAR configuration), the following workflow is executed:

1 Update Phone CSS to the original CSS.
2 Update Line Partition and CSS to the original values.
3 Delete the Hotdial Translation pattern.
4 Delete the Hotdial CSS.
5 Delete the Hotdial Route Partition.
6 For SIP Phones only, the device is updated to use a Dial Rule of "None", and the Dial Rule is deleted.

**Hunt Group Management**

Hunt Groups are relevant to Sites only, and can be configured by a site administrator, or higher level administrator who must first navigate to the relevant site hierarchy.

The purpose of hunt group management is to provide business context for the lines selected as members of line groups and to provide the user with a single consolidated view of the following hunting elements.

- Hunt Pilot
- Hunt List
- Line Groups

All fields of the hunt pilot and hunt list are mapped to the user input. Note that not all hunt group fields are exposed to the Site Admin. The user must select the lines that belong to line groups or any existing line groups that must be added to the hunt list members.

Searches can be performed on any of the details of the hunt pilot.

A hunt group is a combination of the above elements that are automatically linked together using unique identifiers for the following:
• The hunt pilot's hunt list is set to the name of the hunt list. Note that the hunt list name must be configured first in order for it to appear in the hunt pilot tab.

• The hunt list's line group members is set to the name of the associated line groups.

Certain default values for hunt groups are populated by the site defaults menu item, which can be viewed and edited (depending on your log in level). Go to Dialplan Management > Site Defaults and click on the required site name in the list view.

Hunt groups can be:

• Added - where the user specifies the parameters of the hunt pilot and the hunt list, and selects one or more new or pre-existing line groups. If your administrator has enabled the number inventory feature, the Hunt Pilot Pattern can be selected from a drop-down list of available numbers. If the feature is disabled, the Hunt Pilot Pattern field is a free text field or a drop-down containing only selected available numbers. To allow the successful use of call forwarding in a hunt pilot, the defaults for Max Callers In Queue (32) and Max Wait Time In Queue (900) are cleared to allow the successful use of call forwarding in a hunt pilot. To use queueing instead of call forwarding, set these values other than the default, for example to 33 and 901.

• Modified - where the user modifies the parameters of the hunt pilot or hunt list, for example by adding or deleting additional line groups, and adding or deleting line group members.

• Deleted - where the user deletes a hunt group.

Hunt Group Management Workflows

When adding a new Hunt Group, the following workflow is executed:

1. A hunt pilot is added with the details input by the user.
2. A hunt list is added with the details input by the user.
3. One or more line groups are created with the specified directory numbers as members.

When modifying a Hunt Group, the following workflow is executed (depending on what was modified):

1. The line group details are modified.
2. Added line groups are added. Note that removed line groups are not deleted.
3. The hunt list is modified.
4. The hunt pilot is modified.

When deleting a Hunt Group, the following workflow is executed:

1. The line groups that are members of the hunt list are deleted (if they are not used by any other hunt list in the system).
2. The hunt pilot is deleted.
3. The hunt list is deleted.
Call Pickup Groups

Certain default values for call pickup groups are populated by the site defaults menu item, which can be viewed and edited (depending on your log in level). Go to Dialplan Management > Site Defaults and click on the required site name in the list view.

The Call Pickup Groups feature provides an administrator with the following:

• A single interface on which to create call pickup groups, and to select one or more lines as members of a pickup group.

• The ability to add Unified CM call pickup groups and to modify the call forward and call pickup settings of each Unified CM directory number for membership to a newly added call pickup group. When adding a call pickup group, if your administrator has enabled the number inventory feature, the Pattern can be selected from a drop-down list of available numbers. If the feature is disabled, the Pattern field is a free text field or a drop-down containing only selected available numbers.

• The ability to add lines to an existing call pickup group by selecting the pattern (directory number). When adding a member line, if your administrator has enabled the number inventory feature, the Pattern can be selected from a drop-down list of available numbers. If the feature is disabled, the Pattern field is a free text field or a drop-down containing only selected available numbers. The Route Partition Name field is populated automatically based on the selected Pattern.

• The ability to delete a pre-existing call pickup group, and to delete one or more lines from an existing call pickup group.

The first member of the associated pickup group name is set the newly created pickup group, and associated pickup groups can be added as part of the workflow.

Call Pickup Groups Management

When creating a Call Pickup Group, the following workflow is executed:

1  Adds a Unified CM Call Pickup Group.
2  Modifies the Call Forward and Call Pickup Settings of each line by setting the Call Pickup Group to the newly created Call Pickup Group.

When deleting a Call Pickup Group, the following workflow is executed:

1  All lines belonging to the call pickup group are updated to remove them from the call pickup group.
2  All associated pickup groups are modified to remove the call pickup group associations to the deleted call pickup group.
3  The call pickup group is deleted from Unified CM.

When modifying a Call Pickup Group:

• A change to the name of the Call Pickup Group also requires a corresponding change to the name in the list of Included Call Pickup Groups.
Services

- Voice Mail, page 203
- Setup Contact Center Using Cisco Unified Communications Manager, page 209

Voice Mail

Create Voice Mail Service

Before You Begin

To associate Voice Mail Service with a Cisco Unified Communications Manager, you need to know the SIP trunking endpoint information between the Voice Mail Server and the Cisco Unified Communications Manager before starting this procedure.

A Cisco Unity Connection server must be configured before performing this procedure. For procedures, refer to Cisco Hosted Collaboration Solution, Release 10.6(1) Customer Onboarding Guide.

Procedure

Step 1 Log in as the Provider or Reseller Administrator.

Step 2 Make sure the hierarchy path is set to the correct provider, reseller, or customer node.
If the voice mail server is shared by multiple customers configure the service at the provider or reseller level.
If the voice mail server is dedicated to a single customer, configure the service at the customer level.

Step 3 Select Services > Voice Mail > Voice Mail Service.

Step 4 Click Add to add a Voice Mail Service.

Step 5 Enter a Voice Mail Service Name if desired. Do not add spaces in the name.

Step 6 From the Voice Mail Cluster pulldown menu, select the name of the server for voice mail service.

Note The Cisco Unity Connection server must be previously defined under the Provider level at Device Management > CUCs. This is also the location whether the Voice Mail server in a multi-tenant environment is categorized as Dedicated or Partitioned. This determines what elements are available to the Voice Mail Server, whether an additional tenant should be created on the Voice Mail Server, and so on.
Step 7  To integrate the Voice Mail Service with Cisco Unified Communications Manager, click the **Integrate with CUCM** box. Default is unchecked.

Step 8  If the Voice Mail Service is managed by a Cisco Unified Communications Manager, select the Cisco Unified Communications Manager to be paired with the Voice Mail Unity Server from the **CUCM Cluster** pulldown menu.

**Note**  The Cisco Unified Communications Manager must be previously defined under the Provider level at **Device Management > CUCMs**.

Step 9  Complete the SIP trunk provisioning information (between the SIP trunk and the Cisco Unity Connection server) in the following fields:

a) Enter the hostname or IP address of the Voice Mail Server trunk in the **Voice Mail Trunk Address** field.

b) Enter the Voice Mail Server port number (1 to 65535) in the **Voice Mail Trunk Port** field.

**Note**  Do not specify port 5061, which is reserved for secure SIP.

c) Enter the hostname or IP address for the Voice Mail Server to reach the Cisco Unified Communications Manager in the **Remote Trunk Address** field.

d) Enter the Cisco Unified Communications Trunk port number in the **Remote Trunk Port** field.

**Note**  Do not specify port 5061, which is reserved for secure SIP.

**Note**  Only one Cisco Unified Communications Manager and one Cisco Unity Connection can be specified here. To support redundancy and failover in a multinode configuration, the trunk information must be manually updated on the UC apps.

Step 10  In the **Voice Messaging Ports** field, enter the number of voice messaging ports to be created for the voice mail service and associated with the appropriate Port Group on Cisco Unity Connection when the voice mail service is associated to a customer.

Valid values are 1–250. The default is 3. This field is mandatory.

**Note**  The number of voice messaging ports that you add cannot bring the total number of voice messaging ports for all port groups to more than the maximum number of voice messaging ports that are enabled by the Cisco Unity Connection license files. If the license files do not enable the total number of ports, you will not be able to add the new ports.

Step 11  Click **Save** to add the Voice Mail Service you defined.

When a shared Voice Mail Service is created and "Integrate with CUCM" is selected, the following occurs:

- **In Cisco Unified Communications Manager**: Cluster-level SIP Trunk and Route Group is provisioned for the shared voice mail service.
- **In Cisco Unity Connect**: Cluster-level Port Group appears on the PhoneSystem for the shared voice mail service.

---

**What to Do Next**

Perform **Associate Voice Mail Services to Customer**, on page 205.
Associate Voice Mail Services to Customer

Before You Begin

- To associate Voice Mail Service with a customer, the Voice Mail Service must be created before starting this procedure. See Create Voice Mail Service, on page 203.
- If the “Integrate with CUCM” option was selected when the Voice Mail services was created, a customer dial plan and a site dial plan must be created before a Voice Mail Service can be associated with a customer; otherwise the association will fail.

Procedure

| Step 1 | Log in as the Provider or Reseller Administrator. |
| Step 2 | Set the hierarchy path to the customer to which you want to associate the Voice Mail Service. |
| Step 3 | Select Services > Voice Mail > Associate Voice Mail Service to Customer. |
| Step 4 | Click Add to associate Voice Mail Service to a customer. |
| Step 5 | From the Voice Mail Service pulldown menu, select the name of the Voice Mail Service that has been defined by the provider and available to this customer. |
| Step 6 | Click Save to associate the Voice Mail Service with the customer. |

The association appears in the list. When Voice mail Service is associated with a customer and the "Integrated with CUCM" option was selected for the Voice Mail Service, the following is provisioned based on the deployment mode of the voice mail server:

<table>
<thead>
<tr>
<th>Voice Mail Deployment Mode</th>
<th>Cisco Unified Communications Manager</th>
<th>Cisco Unity Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated</td>
<td>Creates Integration at customer level: SipTrunk, Route Group, AllowVm route partition</td>
<td>Creates customer-specific Port Group, ports (3), route partition, calling search space and user template</td>
</tr>
<tr>
<td>Partitioned</td>
<td>Creates Integration at customer level: SipTrunk, Route Group, AllowVm route partition</td>
<td>Creates new tenant (partition), port group, ports (3), route partition, calling search space and user template</td>
</tr>
</tbody>
</table>

Note: The deployment mode for the voice mail service is determined by the mode selected when the Cisco Unity Connection is first added to the Cisco Unified Communications Domain Manager 10.6(1) using Device Management > CUCs.
Add Alternate Extension

Procedure

Step 1  Log in and navigate to the customer level hierarchy.
Step 2  Select Subscriber Management > Voicemail.
Step 3  Enter the account information.
Step 4  Click on the Alternate Extensions tab and select the +.
Step 5  Enter the user Number, Phone type, and Name.
Step 6  Click Save.
Step 7  Log into Cisco Unity Connection.
Step 8  Select the User you have been updating.
Step 9  Select Edit > Alternate Extensions.
        The Alternate Extension will be in place if configured from Cisco Unified Communications Domain Manager 10.6(1).
Step 10 From Alternate Extension select the drop down for Partition and click Save.

Add Additional Notification Devices

Procedure

Step 1  Log in and navigate to the Customer Level Hierarchy.
Step 2  Select Subscriber management.
Step 3  Select Voicemail > Notification Devices.
Step 4  Click the Phone and + buttons.
Step 5  Select Client Work. Click Active and add the phone number. That number will be configured to receive additional notifications.
Disassociate Voice Mail Services from Customers

Procedure

Step 1 Log in as the Provider Administrator.
Step 2 Set the hierarchy path to the customer from which you want to disassociate the Voice Mail Service.
Step 3 Select Services > Voice Mail > Associate Voice Mail Service to Customer.
Step 4 From the list of associations, choose the Voice Mail Service customer association to be deleted, by clicking on its box in the leftmost column.
Step 5 Click Delete to disassociate the Voice Mail Service from the customer.
Step 6 From the popup window, click Yes to confirm the change.
When the delete action is complete, the Voice Mail Service association to the customer disappears from the list.

Delete Voice Mail Service

Procedure

Step 1 Log in as the Provider Administrator.
Step 2 Select Services > Voice Mail > Voice Mail Service.
Step 3 From the list of Voice Mail Services, choose the service to be deleted, by clicking on its box in the leftmost column.
Step 4 Click Delete to delete the Voice Mail Service.
Step 5 From the popup window, click Yes to confirm the deletion.
When the delete action is complete, the Voice Mail Service disappears from the list.

Define a Voice Mail Pilot Number

Before You Begin
To create one or more Voice Mail Pilot Numbers for Voice Mail Services that have previously been associated with the customer, the following procedures must be completed before performing this procedure:

- Voice Mail Service must be created. See Create Voice Mail Service, on page 203.
- Voice Mail Service must be associated with the customer. See Associate Voice Mail Services to Customer, on page 205.
## Associate Pilot Numbers to a Site

### Before You Begin

- To associate Voice Mail Pilot number with a customer, the Pilot Number must be created before starting this procedure. See Define a Voice Mail Pilot Number, on page 207.

### Procedure

**Step 1** Log in as a Customer or Provider administrator.

**Step 2** Set the hierarchy path to the desired Site.

**Step 3** Select Services > Voice Mail > Associate Pilot Number to Site.

**Step 4** Click Add to associate a Voice Mail Pilot Number with a site.

**Step 5** From the Voice Mail Service pulldown menu, select the name of the Voice Mail Service.

**Step 6** From the Voice Mail Service Pilot Number pulldown menu, select the Pilot Number for the selected Voice Mail Service.

**Step 7** Click Save to associate the Voice Mail Service Pilot Number with the site.

### Voice Mail Deployment Mode

<table>
<thead>
<tr>
<th>Voice Mail Deployment Mode</th>
<th>Cisco Unified Communications Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated</td>
<td>At customer level: Route List, Route Pattern, CSS, Voice Mail Pilot, Voice Mail Profile</td>
</tr>
<tr>
<td>Partitioned</td>
<td>At customer level: Route List, Route Pattern, CSS, Voice Mail Pilot, Voice Mail Profile</td>
</tr>
</tbody>
</table>

---

### Cisco Unified Communications Domain Manager, Release 10.6(1) Maintain and Operate Guide

---
The association appears in the list. When a pilot number is associated to a site, the Site Management > Defaults > CUC Defaults are updated so that the subscriber management templates can take advantage of this new voice mail service for the site.

## Disassociate Pilot Numbers from a Site

**Procedure**

**Step 1** Log in as the Customer Administrator. For a list of the roles and tasks that can be done at each level, see Cisco Hosted Collaboration Solution Roles and Privileges, on page 44.

**Step 2** Select Services > Voice Mail > Associate Pilot Number to Site.

**Step 3** From the list of associations, choose the Pilot Number association to be deleted, by clicking on its box in the leftmost column.

**Step 4** Click **Delete** to disassociate the Pilot Number from the site.

**Step 5** From the popup window, click **Yes** to confirm the change. When the delete action is complete, the Pilot Number association to the site disappears from the list.

## Delete a Voice Mail Pilot Number

**Procedure**

**Step 1** Log in as the Customer Administrator. For a list of the roles and tasks that can be done at each level, see Cisco Hosted Collaboration Solution Roles and Privileges, on page 44.

**Step 2** Select Services > Voice Mail > Pilot Numbers.

**Step 3** From the list of Pilot Numbers, choose the number to be deleted, by clicking on its box in the leftmost column.

**Step 4** Click **Delete** to delete the Voice Mail Pilot Number.

**Step 5** From the popup window, click **Yes** to confirm the deletion. When the delete action is complete, the Voice Mail Pilot Number disappears from the list.

## Setup Contact Center Using Cisco Unified Communications Manager

Contact Center provisioning configures Cisco Unified Communications Manager to communicate with Contact Center.
Configure Services > Contact Center > Servers to enable Cisco Unified Communications Manager to communicate with Contact Center when transferring a call from agent to agent and routing a call back to the Customer Voice Portal (CVP).

Configure Services > Contact Center > Service to allow internal service calls to be routed to the CUBE for Contact Center to process.

## Set Up Contact Center Server

### Procedure

**Step 1** Login as a Provider Admin at the Customer hierarchy.

**Step 2** Navigate to Services > Contact Center > Servers menu to add a Contact Center server.

**Step 3** Click on Add button to add a new Contact Center server and fill in the fields and save the Contact Center server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact Center Server Name</strong></td>
<td>Unique server name. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Server description.</td>
</tr>
<tr>
<td><strong>Cisco Unified Communication Manager</strong></td>
<td>The Cluster you want to use for Contact Center Server. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Transfer Conference Pattern</strong></td>
<td>Transfer conference pattern used when transferring calls between agents. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Network VRU</strong></td>
<td>Pattern used to route calls to a CVP. This field is mandatory.</td>
</tr>
<tr>
<td><strong>Trunk Destination Type</strong></td>
<td>CVP or CUBE or CUSP SIP Trunk. This field is mandatory. <strong>Note</strong> Both CVP and CUBE trunks must be added for this Contact Center Server to be added successfully.</td>
</tr>
<tr>
<td><strong>Trunk Destination Address</strong></td>
<td>The destination address of the CVP or CUBE or CUSP SIP Trunk. This field is mandatory. Multiple destination addresses &amp; ports can be added for each trunk type.</td>
</tr>
<tr>
<td><strong>Trunk Destination Port</strong></td>
<td>The destination port of the CVP or CUBE or CUSP SIP Trunk, if no value provided system takes 5060 as default.</td>
</tr>
<tr>
<td><strong>Trunk Security Profile</strong></td>
<td>The SIP trunk Security Profile that needs to be used by each trunk. This field is mandatory.</td>
</tr>
<tr>
<td><strong>SIP Profile</strong></td>
<td>The SIP trunk profile that needs to be used by each trunk. This field is mandatory.</td>
</tr>
</tbody>
</table>
For 500/1000/4000/12K/SCC - You must provide information for a CVP and a CUBE SIP Trunk. For Small Contact Center, both the CVP and CUBE trunks should have the same IP address with a different Trunk Security Profile selected in the **Trunk Security Profile** drop-down for each trunk.

For CUSP - You must provide information for a CUSP SIP Trunk. Only one trunk type can be added.

**Note**  
For CUSP, use only one SIP trunk. For CVP or CUBE, use two SIP trunks.

1. Device Poll will create automatically as a part of Contact Center server with the name "Cu<CUSTOMER_ID>-CC<CC_SERVER_ID>-DP" with the default Call Manager Group & Region.
2. Call Manager Group & Region can be changed in the Cisco Unified Communication Manager as desired.
3. Two application users creates with names pguser & pguser2 - both are created with default password "cisco".

**Note**  
- Planning to change the pguser & pguser2 names to tie with the Customer ID in future releases.
- For all the phone line CSS of a site, add Cu<CUSTOMER_ID>-CC<CC_SERVER_ID>-Xfer4CCServer-PT to the Class of Service member list as a partition with the next available index.
- The admin needs to add **Default Region** as **related regions** for each site region created for a site.
- Reset the trunk by clicking the **Reset** button in the **Trunk** page after updating the SIP profile.

---

## Set Up Contact Center Service

**Procedure**

**Step 1**  
Log in as a Provider Admin at the Customer hierarchy.

**Step 2**  
Navigate to **Services > Contact Center > Services** menu to add a Contact Center Service.

**Step 3**  
Click on **Add** button to add a new Contact Center Service, fill in the fields, and save.

**Note**  
- Customer & Site Dial Plan is required to add a Contact Center Service.
- Only ONE instance of Contact Center Server can be created for a Cisco Unified Communications Manager cluster.
- Only ONE instance of Contact Center Service can be created for a Contact Center Server.
- For CUSP only ONE trunk of type CUSP needs to be added.
- For deleting a server, ensure the service is deleted first.
Configure Unified Mobile Agent

Configure CTI Port

Procedure

Step 1 Select Subscriber Management > Phones.
Step 2 Click Add in the top-right-hand pane to create a new CTI port.
Step 3 Select the Hierarchy Provider > Reseller > Customer > Site.
Step 4 Click the Phone tab, and then select CTI Ports as Product Type.
Step 5 For Device Name, enter a unique name for the Local CTI Port pool name. For example, Use the following format for the device name (LCPxxxxFyyyy):
   • LCP identifies the CTI Port as a local device.
   • xxxx is the peripheral ID for the Unified Communications Manager PIM.
   • yyyy is the local CTI Port.

Step 6 Enter description for the Local CTI Port in the Description field.
Step 7 Select the appropriate device pool from the Device Pool drop-down list
Step 8 Go to the Lines tab.
Step 9 Click + to add a new line.
Step 10 Go to Dirn > Pattern, and select a unique directory number for the CTI port.
Step 11 Click Save.
   Ensure that you leave all the fields with default values in this page.

Step 12 Select Subscriber Management > Phones.
Step 13 Click Add in the top-right-hand pane to create a new CTI port.
Step 14 Select the Hierarchy Provider > Reseller > Customer > Site.
Step 15 Click the Phone tab, and then select CTI Ports as Product Type.
Step 16 In the Device Name field, enter a unique name for the Local CTI Port pool name.
Step 17 For Device Name, enter a unique name for the Local CTI Port pool name. For example, Use the following format for the device name (RCPxxxxFyyyy):
   • RCP identifies the CTI Port as a Network device.
   • xxxx is the peripheral ID for the Unified Communications Manager PIM.
**Configure Cisco Media Sense**

**Setup Trunk**

*Procedure*

- **Step 1** In the **Unified Communications Domain Manager**, select **Device Management > CUCM > Select SIP Trunks**.
- **Step 2** Click Add.
- **Step 3** In the **Device Information** tab, select CUCM from the drop-down list.
- **Step 4** Enter device name in the Device Name field.
  - This is a mandatory field when you add a trunk, but a Read-Only field when you modify a trunk.

---

**Tag CTI Port as Contact Center Agent Line**

*Procedure*

- **Step 1** Select **Subscriber Management > Agent Lines**.
- **Step 2** Select **Hierarchy Provider > Reseller > Customer > Site**.
- **Step 3** Click **Add** in the top-right-hand pane to create a new CTI port.
- **Step 4** Select **Phone** from the **Device Type** drop-down list.
- **Step 5** Click on the port name, and then, select a port from the list of Phone Name.
- **Step 6** Select the Line from the **Line** drop-down list.
- **Step 7** Select **pguser** from the **Application User** drop-down list.
- **Step 8** Click **Save**.
- **Step 9** Repeat the steps for both LCP and RCP ports.

---

- yyyy is the Network CTI Port.

**Step 18** Enter description for the Local CTI Port in the **Description** field.

**Step 19** Select the appropriate device pool from the **Device Pool** drop-down list.

**Step 20** Go to the **Lines** tab.

**Step 21** Click + to add a new line.

**Step 22** Go to **Dirn > Patern**, and select a unique directory number for the CTI port.

**Step 23** Click **Save**.

Ensure that you leave all the fields with default values in this page.
Step 5  Enter description in the Description field.
Step 6  Go to SIP Info tab, and click + to add trunk destination.
Step 7  Enter Ipv4 Address of Media Sense Server, Port, and Sort Order.
Step 8  Click Save.

Setup Route Group

Procedure

Step 1  In the Unified Communications Domain Manager, select Device Management > CUCM > Route Groups.
Step 2  Click Add.
Step 3  Select CUCM from the drop-down list.
Step 4  Enter route group name in the Route Group Name field.
Step 5  Select Distribution Algorithm.
Step 6  Click + to add Trunk under Members.
Step 7  Select Trunk from drop-down list for the Device Name.
Step 8  Click Save.

Setup Route List

Procedure

Step 1  In the Unified Communications Domain Manager, select Device Management > CUCM > Route Lists.
Step 2  Click Add.
Step 3  Select CUCM from the drop-down list.
Step 4  Enter Route List Name, Description, and Call Manager Group Name.
Step 5  Check the Run on Every Node checkbox if you want the route list to be active on every node.
Step 6  In the Route Group Items, click + to add route group.
Step 7  Select route group from the Route Group drop-down list.
Step 8  Click Save.
**Setup Route Patterns**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the <strong>Unified Communications Domain Manager</strong>, select <strong>Device Management &gt; CUCM &gt; Route Lists</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select CUCM from the drop-down list, and then, enter route pattern name and description.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select <strong>Route Partition</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From <strong>Destination</strong>, select either Route List or Gateway/Trunk from the drop-down list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**Configure Device**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the <strong>Unified Communications Domain Manager</strong>, select <strong>Subscriber Management &gt; Phones</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>audio forking phone configured</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Built-In-Bridge</strong> configuration for the device, and change the setting to <strong>ON</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select <strong>Line details</strong> from the <strong>Line</strong> tab.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter the recording profile created using CUCM in <strong>Recording Profile Name</strong> field. If using a recording partner, select <strong>Automatic Call Recording Enabled</strong> from the <strong>Recording Flag</strong> drop-down list, as per the recording partner recommendations. If not using a recording partner, select <strong>Automatic Call Recording Disabled</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
Set up Cisco Remote Silent Monitoring

Create Unified CM Group

Procedure

Step 1
Select the customer in the hierarchy.

Step 2
Select **Device Management > CUCM > Unified CUCM Group**.

Step 3
Select the appropriate NDL from the drop-down list to add a new region, and click **OK**.

Step 4
Enter **RSMSimPhone** for the Unified Communication Manager group name.

Step 5
Add **UCM Group Item**, and then give priority.

Step 6
Select **Cisco Unified Communication Managers** from the drop-down.

Step 7
Click **Save**.

Create Region

Procedure

Step 1
Select the customer in the hierarchy.

Step 2
Select **Device Management > CUCM > Region**

Step 3
Select the appropriate NDL from the drop-down list to add a new Region, and then, click **OK**.

Step 4
Select **CUCM** from the drop-down list.

Step 5
Enter **AR_RSMSimPhone** as the region name.

Step 6
Add **Related Region**, and then, complete the following fields:
   a) Select **Audio Bandwidth** value as 64.
   b) Select the appropriate **Immersive Video Bandwidth** from the drop-down list.
   c) Select the appropriate **Video Bandwidth** from the drop-down list.
   d) Select the appropriate **Region name** from the drop-down list.

Step 7
Click **Save**.
Create Device Pool

Procedure

**Step 1** Select the customer in the hierarchy.
**Step 2** Select Device Management > CUCM > Device Pool.
**Step 3** Select the appropriate NDL from the drop-down list to create a new device pool, and then, click OK.
**Step 4** Enter the device pool name as RSMSimPhone_DP.
**Step 5** Select RSMSimPhone from Unified Communication Manager Group drop-down list.
**Step 6** From the Roaming Sensitive Settings tab, select the appropriate date/time group from the drop-down list.
**Step 7** Select AR_RSMSimPhone from the Region drop-down list.
**Step 8** Select SRST Reference as Disable.

Create Phones

Procedure

**Step 1** Select the customer in the hierarchy.
**Step 2** Select Subscriber Management > Phones, and then, click Add.
**Step 3** Click the Phone tab.
**Step 4** Enter the device name and add SEP before the mac address. For example, if the mac address is 000000000AB1 the device name must be SEP000000000AB1.
**Step 5** Select the Product Type as 7941.
**Step 6** (Optional) Enter the phone description.
**Step 7** From the Device Protocol, select SIP from the drop-down list.
**Step 8** From the Device Pools Name, select RSMSimPhone_DP from the drop-down list.
**Step 9** Click the Line tab.
**Step 10** Click the + symbol.
**Step 11** Select the directory number from Pattern drop-down list.
**Step 12** Set the Monitoring Calling Search Space as the CSS that is configured in the Calling Search Space field in the Lines page.
**Step 13** Enter Busy Trigger value as 1, and the Maximum Number Call as 2 in the text box.
Self Provisioning Overview

The Cisco Unified Communications Manager Self-Provisioning feature allows an end user or administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user. The following process is used to self-provision a phone:

1. The user or admin connects the phone to the network.
2. The phone auto-registers.
3. The user or admin dials the IVR application and satisfies the prompts.
4. The IVR application deletes the auto-registered phone and adds it back using templates associated with the user via their User Profile.

There are two requirements related to self-provisioning:
1 Before a phone can be self-provisioned, the user must exist in Cisco Unified Communications Manager along with their primary extension, self-service ID, and user profile.

2 After the phone is self-provisioned, in order to do additional subscriber management for the user in Cisco Unified Communications Domain Manager, the user, line, and phone need to be at the site level in the Cisco Unified Communications Domain Manager hierarchy.

**Bottom-Up User Management**

A **bottom-up** approach to user management means users are configured on Cisco Unified Communications Manager and synced into Cisco Unified Communications Domain Manager. Two possible methods for bottom-up user management are:

- Sync LDAP directory into Cisco Unified Communications Manager. Do not configure the LDAP directory sync in Cisco Unified Communications Manager to use a line mask or DN pool to create the user's primary extension. Instead, the user's primary extension and self-service ID are generated in Cisco Unified Communications Domain Manager, using a line mask, universal line template, and self-provisioning user profile at the site level.

  ![Note](note)

  During LDAP sync to Cisco Unified Communications Manager, the user is assigned a User Profile via the Feature Group Template associated with the LDAP directory. In order for the line mask configured at the site on Cisco Unified Communications Domain Manager to get applied, the User Profile assigned previously must be empty or it must be named the 'Standard (Factory Default) User Profile'.

  - Use Cisco Unified Communications Manager Quick User/Phone Add to create a user and the user's primary extension.

  See Cisco Unified Communications Manager documentation for more information.

**Top-Down User Management**

A **top-down** approach to user management means users and lines are configured on Cisco Unified Communications Domain Manager and pushed into Cisco Unified Communications Manager. Users may be added via LDAP sync, the GUI, or bulk loading. When users are pushed to Cisco Unified Communications Manager the user's primary extension is created, and when a phone is self-provisioned for the user, the phone is automatically moved to the user's Site.

Use either of the following methods to configure the user in Cisco Unified Communications Domain Manager:

- Generate the user's primary line and self-service ID using a line mask, universal line template, and a user profile at the site level.

- Set the self-service ID per user using Quick Add Subscriber.
Using a combination of the methods above is possible but is not recommended. For example, you can enable the line mask at the site and use Quick Add Subscriber to set the primary line for some users while not setting it for others. When the line mask is applied, it first checks to see if a primary extension is already assigned to the user (perhaps via Quick Add Subscriber). If a primary extension is already assigned, the line mask is not applied.

Cisco Unified Communications Manager Configuration for Self-Provisioning

To use self-provisioning, regardless of whether top-down or bottom-up user management is used, the following one-time configuration tasks must be done on Cisco Unified Communications Manager:

- Ensure that the Cisco CallManager, Cisco CTIManager, and Self-Provisioning IVR services are activated
- Configure Auto Registration
- Configure an Application User and credentials so the system can connect to the IVR self-provisioning service
- Configure a CTI Route Point (this provides the number that users dial to connect to the IVR)
- Configure Self-Provisioning with the Application User and CTI Route Point

Site Configuration for Self-Provisioning

Regardless of whether top-down or bottom-up user management is used, ensure that the following items have been configured in Cisco Unified Communications Domain Manager:

- Site Dial Plan: Dial Plan Management > Site > Dial Plan
- Site Defaults: Site Management > Defaults
- Directory Number Inventory: Dial Plan Management > Customer Management > Add Directory Number Inventory

Generate User's Primary Line

If top-down user management is used, when the users are pushed to Cisco Unified Communications Manager, the system automatically creates the user's primary line, associates the line as the primary extension, sets the self-service ID, and sets the user profile.

If bottom-up user management is used, the user's primary line is created (if it doesn't already exist) when the user is moved to a site, or updated once at a site.

The line is created by applying the Line Mask to a user attribute (typically the user's telephone number) and using the Universal Line Template (ULT) to determine the route partition name and other line attributes. The
ULT is specified in the Self-Provisioning User Profile which is specified in the Site's Default User Profile. For this approach the admin needs to configure the following at the site level:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure Universal Device Template(s). See Add Self-Provisioning Universal Device Template, on page 222.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure Universal Line Template(s). See Add Self-Provisioning Universal Line Template, on page 224.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure Self-Provisioning User Profile(s). See Add Self-Provisioning User Profile, on page 225.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure a Site Default User Profile. See Set Default User Profile for Site, on page 225.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure Line Mask. See Add Self-Provisioning Line Mask, on page 226.</td>
</tr>
</tbody>
</table>

### Specify the Primary Line per Subscriber

In the top-down method that uses Quick Add Subscriber, the primary line pattern is specified by the admin. This creates the user's primary line, associates it as the primary extension, sets the self-service ID, and sets the user profile. The line attributes come from Quick Add Group configuration. Therefore, the Universal Line Template does not need to be configured.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure Universal Device Template(s). See Add Self-Provisioning Universal Device Template, on page 222.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure Self-Provisioning User Profile(s). See Add Self-Provisioning User Profile, on page 225.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure a Site Default User Profile. See Set Default User Profile for Site, on page 225.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure primary line per user. For Quick Add Subscriber, add at least one line, and check the Self-Service ID checkbox.</td>
</tr>
</tbody>
</table>

### Add Self-Provisioning Universal Device Template

When the administrator or user self provisions a phone, Cisco Unified Communications Manager deletes the auto registered phone and re-adds the phone back into the database. The various phone settings for the user's phone are determined by the Universal Device Template (UDT) associated with the user's User Profile.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in as provider, reseller, or customer admin.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Set the hierarchy path to the site node where you want to configure self-provisioning.</td>
</tr>
</tbody>
</table>
**Step 3** Select **User Management > Self-Provisioning > Universal Device Template**.

**Step 4** Click **Add**.

**Step 5** Enter the following required Universal Device Template information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the universal device template</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>Common Phone Profile</td>
<td>Select a common phone profile from the drop down list.</td>
</tr>
<tr>
<td>Phone Personalization</td>
<td>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.</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.</td>
</tr>
<tr>
<td>Max 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.</td>
</tr>
<tr>
<td>MultiLevel Precedence and Preemption</td>
<td>This setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call.</td>
</tr>
<tr>
<td>Do Not Disturb Option</td>
<td>When you enable DND on the phone, this parameter allows you to specify how the DND features handle incoming calls.</td>
</tr>
<tr>
<td>Blf Presence Group</td>
<td>Enter the presence group applicable for busy lamp field buttons.</td>
</tr>
<tr>
<td>Device Mobility Mode</td>
<td>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.</td>
</tr>
</tbody>
</table>

These fields may be pre-populated depending on customer, site, and dial plan configuration:

- Name
- Location
- Common Phone Profile
Add Self-Provisioning Universal Line Template

In terms of self-provisioning a phone, the Universal Line Template (ULT) is used before self-provisioning actually takes place. ULTs are used to create directory numbers on Cisco Unified Communications Manager. A directory number is identified by a pattern (the number portion) and a route partition. A directory number also has a variety of settings that can be configured for the line. When a directory number is created using a ULT, the ULT determines the route partition along with the line settings.

Procedure

Step 1 Log in as provider, reseller, or customer admin.
Step 2 Set the hierarchy path to the site node where you want to configure self-provisioning.
Step 3 Select User Management > Self-Provisioning > Universal Line Template.
Step 4 Click Add.
Step 5 Enter the following required Universal Line Template information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the universal line template</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>Partition</td>
<td>Enter the route partition used to create lines at the site.</td>
</tr>
</tbody>
</table>
Add Self-Provisioning User Profile

Procedure

Step 1 Log in as provider, reseller, or customer admin.
Step 2 Set the hierarchy path to the site node where you want to configure self-provisioning.
Step 3 Select User Management > Self-Provisioning > User Profile.
Step 4 Click Add.
Step 5 Enter user profile information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the user profile. This field is mandatory.</td>
</tr>
<tr>
<td>Universal Line Template</td>
<td>Enter a site-specific ULT. This field is highly recommended.</td>
</tr>
</tbody>
</table>

Step 6 Click Save.
Step 7 Enter other optional settings, if applicable.

What to Do Next

Set Default User Profile for Site, on page 225

Set Default User Profile for Site

Set a default User Profile for the site, which will be used when no user profile is specified when adding a subscriber. To set the default User Profile:
Procedure

Step 1 Select Site Management > Defaults.
Step 2 Click the Defaults to edit.
Step 3 Enter the default User Profile for the site in the Default User Profile (for User Self Provisioning) field.
Step 4 Click Save.

Add Self-Provisioning Line Mask

Procedure

Step 1 Log in as provider, reseller, or customer admin.
Step 2 Set the hierarchy path to the site node where you want to configure self-provisioning.
Step 3 Select User Management > Self-Provisioning > Line Mask.
Step 4 Click Add.
Step 5 Provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of the Line Mask.</td>
</tr>
<tr>
<td>User Attribute</td>
<td>Select the user attribute used to generate the user's primary extension. The default is telephoneNumber. This field is mandatory.</td>
</tr>
<tr>
<td>Mask</td>
<td>Provide a mask which gets applied to the user attribute. The result is used as the user's primary extension. For example, assume user attribute is telephoneNumber and the mask is 4XXXX. Special characters and blanks are stripped from the user attribute before applying the mask. If the mask is applied to '(919) 867-5309', the user's primary extension would be set to 45309. This field is mandatory.</td>
</tr>
</tbody>
</table>

Step 6 Click Save.
Customizations

- Common Tasks, page 227
- Role Management, page 230
- GUI Customization, page 235
- Themes, page 235
- Download, Edit and Update a Theme, page 236
- Add a Theme, page 237
- Theme Settings Reference, page 238
- Set the Login Page Theme, page 239
- Menu Layouts, page 239
- Create a Menu Layout, page 240
- Landing Pages, page 241
- Create a Landing Page, page 241
- Landing Page Definition, page 244
- Field Display Policies, page 246
- Clone a Field Display Policy, page 247
- Configuration Templates, page 248
- Clone a Configuration Template, page 249
- Access Profiles, page 250
- Clone an Access Profile, page 250

Common Tasks

The user interface allows for a number of common procedures across all interfaces. This includes item single- and multi-selection, actions on items and ordering or moving items.
Clone

An item instance can be cloned. Cloning provides a quick way to create items or instances that have very similar data.

On the GUI, a clone button is available to carry out the task. This button is available on the specific item page and not on the list of items view.

The cloned item is created in the system only after the user clicks Create on the button bar.

If an item refers to other items, only the current item instance is cloned, and not the referenced items. For example, if a Phone on the system is cloned, the device models (Phone and Remote Destination) that are referred to in this item are not cloned.

The cloned key field(s), for example Name, must be edited with new values to ensure creation of a new item in the system. An error message, “Error, Duplicate Resource Found.” is displayed if a key field is not changed.

Create a Clone

Procedure

Step 1 Choose the hierarchy level of the item or item instance to be cloned.
Step 2 Choose the required item or instance that you want to clone.
Step 3 Click Clone on the button bar.
Step 4 The page refreshes and the form displays the cloned item.
Step 5 Edit the required details, and click Create on the button bar when complete to create the new instance from the clone.

Selecting Items

Items that have already been created can be modified or deleted as required. This can be performed either on single items or multiple items.

Procedure

Step 1 For a single item in the list view, click the required single item that you want to edit or delete.
Step 2 For multiple items in the list view, select the check box for each item that you want to edit or delete. If the list view of items spans more than one page, items can be selected on each page as required.
Step 3 Click Delete or Modify in the button bar to delete or modify the selected items.
Ordering Lists

The list view of items allows for basic ordering by column. The ordering of a column is shown by the up/down arrow.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click in the column header of a list. String columns are sorted alphabetically and numeric columns are sorted numerically.</td>
</tr>
<tr>
<td>2</td>
<td>Click the column header name or up/down arrow to change the direction or the sort order of the column.</td>
</tr>
</tbody>
</table>

Filtering Lists

Cisco Unified Communications Domain Manager 10.6(1) allows you to filter lists in order to view only data based on specific criteria. This includes Transactions and their Sub Transaction and Log lists.

A Filter button is available next to the navigation controls at the bottom of a list. Select the button to open the multi-filter dialog.

A filter instance consists of a selected column, a matching filter type and a value. Values are case insensitive. Filter instance rows can be added or removed on the dialog to create a filter. The combination of instances create a single filter where all instance rows are applied.

To apply the filter, press Enter or select the Apply button. This will hide the active filter dialog and show the filtered list.

For model lists, actions can then for example be carried out on a selection of items from the filtered list. The filter remains active until it is removed or until the user session on the GUI ends.

The Filter button funnel icon is black when a filter is active, and white when no filter is present. A funnel icon also shows in the list header to indicate that a filter is active and that the list is currently filtered.

If a filter is active on a list, select the Filter button to display the multi filter dialog again.

Close an unapplied filter dialog by clicking outside it. Unapplied filters are lost when the dialog is closed.

A filter remains active even when navigating away from the list. More than one filter can be therefore be active on lists available in a session on the GUI.

Remove an active filter by selecting the Remove button on the multi filter dialog or by selecting the X button next to the active Filter button.

Navigating Lists

If a list contains multiple items, page navigation controls at the bottom, center of the screen allow you to:

- scroll to the next/previous page using the right/left arrow respectively.
- scroll to the first or last page of the list as required.
- Go to a specific page by entering the required page number and clicking Go (or pressing Enter).
- Specify the number of items to display on a page, 25 to 200 (in increments of 25).
- If you are unsure of the total number of items in a particular list view, click on the [get total] link.

**Updating on Pop-up Screens**

User interface forms that open pop-up screens to add or delete instances carry out the Add or Delete task when the **OK** button is clicked on the pop-up screen. In these instances, it is not necessary to click the **Modify** button on the parent user interface form to complete the task.

**Role Management**

Provider administrators can manage the roles that are available for administrators, operators, and users at lower levels in the hierarchy.

**Procedure**

1. **Step 1** Log in as a provider admin.
2. **Step 2** Select **Role Management > Roles**
3. **Step 3** To add a new role click the **Add** button.
   a) Enter or select the following role settings:

**Table 7: Role settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the role. This field is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the role.</td>
</tr>
<tr>
<td>Hierarchy Type</td>
<td>The type of hierarchy nodes applicable at the selected hierarchy level. For example, at Provider level, the following values are allowed: Provider, Reseller, Customer, and Site. While at the Reseller level, the following values are allowed: Reseller, Customer, Site. Controls which roles are available at which levels in the hierarchy. Also used with Hcs Component Access and Service Assurance Role Type when mapping roles to HCM-F. This field is mandatory.</td>
</tr>
<tr>
<td>Hcs Component Access</td>
<td>Controls what HCM-F components (FF and/or SA) that users with this role have access to. Used with Hierarchy Type and Service Assurance Role Type when mapping roles to HCM-F. This field is mandatory.</td>
</tr>
<tr>
<td>Access Profiles</td>
<td>Permissions for resources are defined in Access Profiles. This field is mandatory.</td>
</tr>
</tbody>
</table>
### Clone a Role

Use this procedure to clone an existing role for a specific hierarchy node (provider, reseller, customer, or site).

**Procedure**

1. Log in as the hcsadmin or provider administrator.
   - **Note** Administrators can clone roles associated with, or below, their level in the navigation hierarchy.
2. Select Role Management > Roles.
3. Select a role to be cloned by clicking on its box in the leftmost column.
4. Select Action > Clone.
5. Enter a unique name for the role in the Role field. Make the name as descriptive as possible using up to 50 alphanumeric characters, including spaces, period(s), hyphens (-), and underscore characters (_).  
6. (Optional) Add a description for the role in the Description field.
7. Click **Save** to save the role to the hierarchy that appears in the breadcrumb.

### Create a Service Assurance Only Role

To restrict an administrator to performing only service assurance tasks, you need to create the appropriate service assurance only role.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Assurance Role</strong> Type</td>
<td>Controls read/write access to HCM-F components. Used with Hierarchy Type and Hcs Component Access when mapping roles to HCM-F. This field is mandatory.</td>
</tr>
<tr>
<td>Menu Layout</td>
<td>The menu layout assigned to the role. Controls what menu options are available to users assigned to the role.</td>
</tr>
<tr>
<td>Landing Page</td>
<td>The home page assigned with the role. Controls what the home page looks like for users assigned to the role.</td>
</tr>
<tr>
<td>Theme</td>
<td>The name of the theme assigned to the role. The theme controls the overall look and feel of the GUI.</td>
</tr>
</tbody>
</table>
Create a Fulfillment Only Role

To restrict an administrator to performing only fulfillment tasks, you need to create the appropriate fulfillment only role.

Procedure

Step 1 Login as a Provider or hcsadmin administrator.
Step 2 Select Role Management > Roles.
Step 3 Click Add.
Step 4 Enter a name, and optionally a description, for the role.
Step 5 Select the hierarchy type for the role. Controls the hierarchy level that the role is available at.
Step 6 For Hcs Component Access, select Service Assurance Only. The privileges, menu layout, and landing page values are automatically set to the appropriate values for a service assurance only role and cannot be overridden.
Step 7 Optionally, select a theme for the role.
Step 8 Click Save.

Deploy a Customized Credential Policy

A default credential policy called HcsCredentialPolicy is shipped with Cisco Unified Communications Domain Manager 10.6(1). However, a customized credential policy can be deployed at a Provider, Reseller, or Customer hierarchy node.
When a customized credential policy is set as the default credential policy at a hierarchy node, all users and admins at or below that hierarchy node will be subject to the customized credential policy, except for any users or admins that have explicitly been assigned a different credential policy.

**Credential Policy Inheritance**

Unless explicitly assigned a credential policy, users and admins are subject to the default credential policy set at a hierarchy node at or above their location. The default credential policy for the hierarchy node closest to the user or admin location is used. If no customized credential policies have been deployed all users and admins are subject to the HcsCredentialPolicy credential policy which is the default credential policy at the sys.hcs level.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in as the provider, reseller, or customer administrator.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set the hierarchy path to the node where you want to deploy a customized credential policy.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Role Management &gt; Credential Policy</strong>.</td>
</tr>
</tbody>
</table>
| Step 4 | Either clone the HcsCredentialPolicy credential policy, or add a new credential policy:  
  - To clone the HcsCredentialPolicy policy, click HcsCredentialPolicy, then in the Action pulldown, select **Clone**.  
  - To add a new credential policy, click **Add**. The credential policy settings default to the settings for HcsCredentialPolicy. |
| Step 5 | Provide a name for the credential policy. |
| Step 6 | Modify the credential policy settings as needed. |

### Description Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Session Timeout</td>
<td>The number of minutes a user session can be idle before being automatically logged off. The minimum setting is 1 minute and the maximum is 525600 minutes (365 days). The default is 20 minutes.</td>
</tr>
<tr>
<td>Absolute Session Timeout</td>
<td>The number of consecutive minutes a user can be logged in, regardless of session activity, before being automatically logged off. A value of 0 disables absolute session timeout. The maximum is 525600 minutes (365 days). The default is 1440 minutes (24 hours).</td>
</tr>
<tr>
<td>Password Expires</td>
<td>The number of months that can elapse between password resets. The default is 6 months.</td>
</tr>
<tr>
<td>User Must Change Password on First Login</td>
<td>Check this to force users to change password on initial login. The default is disabled.</td>
</tr>
<tr>
<td>Lock Duration</td>
<td>The number of minutes a lock will be held when user is locked out. The default is 30 minutes.</td>
</tr>
<tr>
<td>Disable Failed Login Limiting per User</td>
<td>Check this to not limit the number of times a user can fail to login before the account is locked. The default is to enable the limit.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failed Login Count per User</td>
<td>The number of times a user can fail to login before the account will be locked. The default is 20 times.</td>
</tr>
<tr>
<td>Reset Failed Login Count per User</td>
<td>After this number of minutes from last login attempt, the failed login count will be reset to 0. The default is 5 minutes.</td>
</tr>
<tr>
<td>Disable Failed Login Limiting per Source</td>
<td>Uncheck this to limit the number of times any user from the same IP address can fail to login before the account is locked. The default is to disable the limit. Note: Do not enable source login rate limiting for a credential policy that will apply to Self Service users. A separate credential policy is recommended for administrators and users that do not use Self Service if source login rate limiting is required.</td>
</tr>
<tr>
<td>Failed Login Count per Source</td>
<td>If source login rate limiting is enabled, enter the number of times any user from the same IP address can fail to login before the IP address will be blocked. The default is 10 times.</td>
</tr>
<tr>
<td>Reset Failed Login Count per Source</td>
<td>If source login rate limiting is enabled, this value is the number of minutes from last login attempt from the IP address after which the failed login count will be reset to 0. The default is 10 minutes.</td>
</tr>
<tr>
<td>Number of Questions Asked During Password Reset</td>
<td>Enter the number of security questions a user or admin must answer when resetting their own password via the Forgot Password link. The default is 3.</td>
</tr>
<tr>
<td>Password Reset Question Pool</td>
<td>Contains a list of possible security questions that a user or admin will answer when resetting their own password via the Forgot Password link.</td>
</tr>
</tbody>
</table>

**Note** It is recommended to make credential policy only more restrictive than HcsCredentialPolicy to not invalidate the Cisco Product Security Baseline.

**Step 7** Click **Save**.

**Note** If a user is already logged in when the credential policy is changed, changes do not take effect until the user logs out and logs in again.

**Step 8** Select **Role Management > Default Credential Policy**.

**Step 9** Provide a name for the Default Credential Policy at this hierarchy node.

**Step 10** In the Credential Policy field, select the credential policy you just cloned or added.

**Step 11** Click **Save**.

All users and administrators at or below the hierarchy node will now be subject to the default credential policy, unless the user or admin has been explicitly assigned a credential policy.
Session Timeout Rules

The following rules apply to the idle session timeout and absolute session timeout values that can be applied to users via a credential policy:

- Setting the absolute session timeout to 0 disables it.
- The absolute session timeout takes priority over the idle session timeout. Therefore, setting the absolute session timeout to a value less than the idle session timeout effectively disables the idle session timeout.
- Credential policy session timeouts do not apply to SSO authenticated users. For SSO authenticated users, Cisco Unified Communications Domain Manager honors the SessionNotOnOrAfter SAML 2.0 attribute, which is equivalent to an absolute session timeout, although controlled by the IDP.

GUI Customization

The system allows for the user interface to be customized by a provider administrator (or higher) as required. This customization includes:

- Theme selection
- Menu Layout customization and associated Field Display Policies
- Landing Page customization

Themes

Themes control the look and feel of the entire GUI interface. This contains all aspects of the presentation including the images, logos, colors, fonts, sizing and positioning.

New themes can be added and existing themes can be edited. These are associated with a user's role. There is no limit to the number of themes that can be added and applied. It is a common practice to have a theme associated with a specific customer (company).

The default theme that applies to the GUI when the system is initially built, is available on the system and can be used as the baseline template. The theme is in the form of a Cascading Style Sheet (CSS) to be exported, edited and re-imported as required.

While all aspects of the exported CSS can be modified, we recommend that the default theme is used as a template in terms of basic design in order to prevent usability or functional issues.

The CSS file itself is simple to export and edit. Clear headers in the CSS file indicate which area of the GUI the design applies to. The headers include the following components:

- Navbar
- Shortcut menu
- Hierarchy breadcrumbs
- Quick search
- Tree menu
Images can be stored with the theme or referenced with the use of relative path names.

The theme feature also includes a Use this Theme to style Login page checkbox, which when selected applies the chosen look and feel to the login page across the system. Currently, the system allows only a single theme to be applied to the Login page.

Download, Edit and Update a Theme

**Procedure**

**Step 1** Choose the hierarchy level at which the theme will be applied. Note that themes can only be customized by a Provider Administrator (or higher).

**Step 2** Choose **Role Management > Themes** to open the Themes list view.

**Step 3** Click the theme that you want to download.

**Step 4** Click **Download** on the button bar to download the theme. The exported file is a .zip archive with the name of the theme. The archive contains a folder with the theme name and files called skin.css and skin.less in it.

**Step 5** Refer to the recommended practice to edit the Less file at the end of this topic, otherwise save the file and open the CSS file in a text editor.

- Headers are clearly marked and apply to design areas within the GUI.
- Colors, sizes, fonts, images, and so on, can all be overwritten with the required formats.
- Images must be identified with the correct file path name. Preferably, do not use '/' preceding the path name; rather use relative paths, i.e., a path relative to the CSS file location. For example, if you created an image sub-folder called 'img', use 'img/myimage.png'. After upload, the image should be viewable when opening the URL: http://<hostname>/www/themes/mytheme/img/myimage.png.

**Step 6** When editing is complete, compress the folder and save the file with the .zip file extension. Note that any files or folders inside the zip file archive that start with a '.' character will be silently discarded when unzipping the theme. For example, if the zip archive contains any files named ._.DS_Store or .directory, they will be ignored.

**Step 7** Return to **Role Management > Themes**:

a) For an update, select the theme name and click **Browse** adjacent to Import File and then open the same theme name. Optionally check the **Backup Enabled** check box to create a backup of the current theme on the server. Click **Modify** to complete the import process.

b) For a new theme, enter a theme name that is the same as the new .zip archive filename. Click **Modify** to complete the import process.

c) To delete a theme, select it from the list and click **Delete**.

The preferred way to edit a theme is to edit and compile the Less files. * In addition to the Less files downloaded in the zipped theme, you will need the Cisco Unified Communications Domain Manager 10.6(1) minimal
theme (that can be provided at request) to compile the Less file. It will be included in the downloaded zipped theme automatically in future releases.

- All changes that made directly in the CSS files will have to be manually carried over after each changes in the Less files.
- Edit the Less files and compile them to get the new CSS files.
- The aim with Less is that a theme can be customized with the minimum of technical knowledge.

To compile the Less theme, a Less compiler is required.

**Add a Theme**

**Procedure**

**Step 1**  
Login as hcsadmin.

**Step 2**  
Prepare the theme file  
- Create a folder and add a file skin.css with the required name of the theme. The name of the folder must be the same as the intended theme name (only alphanumeric characters can be used, with no spaces or special characters).
- Add any CSS overrides to the file. Note that only the definitions as shown in the export of a provided CSS file skin.css can be modified.
- Add required image files in this folder (if any).
- Optionally create a settings.json file in the theme folder. The settings.json has flags that controls overall appearance of elements on pages. Refer to the Theme Settings reference topic.
- Create a .zip archive file with the same filename as the folder.

**Step 3**  
Add the theme to the system  
- Choose the hierarchy level at which the theme will be created.
- Choose **Role Management > Themes** to open the Themes list view.
- Click **Add** on the button bar to open the Themes input form. Note that themes can only be customized by a Provider Administrator (or higher).
- Enter the Theme Name (same as the file name created above).
- Click the **Browse** button to import the created theme zip file. Wait until the system displays the file chosen in the **Import File** field.
- If the theme must also apply to the login page, check the "Use this Theme to style Login page" check box.
- Click **Save** on the button bar when complete.

**Theme Field Reference**

<p>| Base |
|------|------|-------|
| Theme Name * | name | The name that is given to the Theme. |</p>
<table>
<thead>
<tr>
<th>Flag Name</th>
<th>Default</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>leftSearch</td>
<td>false</td>
<td>Places search box in the sidebar. When set to true, rightSearch must be false.</td>
</tr>
<tr>
<td>rightSearch</td>
<td>true</td>
<td>Places search box in the right navbar. When set to true, leftSearch must be false.</td>
</tr>
<tr>
<td>fixedNavbar</td>
<td>true</td>
<td>Make navbar sticky at the top of the screen by adding a 'navbar-fixed-top' as class.</td>
</tr>
<tr>
<td>fixedSidebar</td>
<td>true</td>
<td>Make sidebar sticky (always visible).</td>
</tr>
<tr>
<td>fixedBreadcrumbs</td>
<td>true</td>
<td>Make context hierarchy path always visible.</td>
</tr>
<tr>
<td>enableCustomJS</td>
<td>false</td>
<td>Execute custom Javascript that creates a non-native menu scrollbar. Required by the Futurama2 theme.</td>
</tr>
</tbody>
</table>

The contents of a settings.json file with default values looks like:

```json
{
  "leftSearch": false,
  "rightSearch": true,
  "fixedNavbar": true,
  "fixedBreadcrumbs": true,
  "fixedSidebar": true,
  "enableCustomJS": false
}
```
Set the Login Page Theme

**Procedure**

**Step 1** Choose the hierarchy level in which the theme was created or to which the theme belongs.

**Step 2** Choose **Role Management > Themes** to open the Themes list view.

**Step 3** Click the required Theme Name that you want to use for the Login page.

**Step 4** On the **Base** tab, check the Use this Theme to style Login page check box.

**Step 5** On the **Login Page Details** tab, enter the required text in the Title field and Banner text field. The text entered in the Title field will be displayed at the top of the Login page, above the logo. The text entered in the Banner Text field will be displayed at the bottom of the Login page, below the **Log In** button.

**Step 6** Click **Save** on the button bar when complete to implement the selection.

**What to Do Next**

The Login page theme can also be applied to the login page during the log in process. Do this by adding the suffix `?theme=<theme_name>` to the login request url, where `<theme_name>` is an available theme.

**Menu Layouts**

Menu layouts define the view a user has of the menu content and structure on the GUI. This is fully customizable up to three levels deep and can be created or edited to represent the content any user needs to have access to. The association of the defined view of the menu is made with the user's role and menu layouts can be created directly on the GUI.

To refine a view of model entities for a user, a Field Display Policy (FDP) and Configuration Template (CFT) for a model can be applied. The FDP and CFT for a specific model is applied as part of the menu layout - in other words in the menu structure, the FDP and CFT are attributes of the specific model entry for that menu layout. This means that:

- Different FDPs and CFTs for a specific model can define menu layout variations for that model.
- The required FDP and CFT should be available and defined before creating new menus.

Default menu layouts are provided with Cisco Unified Communications Domain Manager 10.6(1). These include defaults for pre-defined hierarchy based user roles, namely HcsAdmin, HcsProviderAdministrator, HcsCustomerAdministrator and HcsSiteAdministrator. The details of these default menu layouts can be viewed and easily edited to either remove or add entries, update entries (for example with an alternative FDP), change default values (for example with an alternative CFT), or change the order and groupings of the items.

The menu layout is an attribute of the user role. Each user must be assigned a User Role, thus the user will see the menu layout based on this user role. Refer to the User Role topic.

Menu layouts can also be copied via the Clone option so they can be edited or exported and re-imported.

Designers who have access to tag or version tag can apply these to a menu layout so that it can be uniquely identified to track and control changes.
Create a Menu Layout

Before You Begin
To work on an existing menu layout, it is recommended to clone the menu layout and work on the clone.

Procedure

Step 1 Login as hcsadmin, provider, or reseller administrator.
Step 2 Choose the hierarchy for the menu layout.
Step 3 From the left menu, select Role Management > Menu Layouts.
Step 4 Click Add.
Step 5 Enter a name and a description for the menu layout.
Step 6 Optionally, click the nest + button on the Menu Items field and fill in data for the necessary fields.
Step 7 Click the Save.

What to Do Next
Assign the Menu Layout to the appropriate Role.

Menu Layout Field Reference

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name *</td>
<td>name</td>
<td>The name that is given to the Menu Layout.</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td>A description of the Menu Layout.</td>
</tr>
<tr>
<td>Menu Items</td>
<td>menu_items</td>
<td>The list of menu items and -sub items that belong to the Menu Layout.</td>
</tr>
</tbody>
</table>

Menu Items

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>title</td>
<td>The menu item title as it will show on the menu.</td>
</tr>
<tr>
<td>Type</td>
<td>type</td>
<td>The selected model type from the Type drop-down list to associate with the Title.</td>
</tr>
<tr>
<td>Href</td>
<td>href</td>
<td>If a direct reference to a model type is used for the menu item, the specified path.</td>
</tr>
</tbody>
</table>
### Landing Pages

This is the user's home page, which is seen when the user logs in and then uses the application **Home** button. The landing page configuration options provide an opportunity to set up short-cut links to frequently used functionality, and to enhance the look and feel on the user's GUI. Images and links can be added in vertical or horizontal patterns with unlimited boxes and shortcuts which can then be assigned to a user's role.

A default page is loaded in the system and associated to pre-defined roles in the hierarchy, for example Provider, Customer, and Site administrators.

These editable configurations provide an easy mechanism to define direct links to areas in the system which can be used as short-cuts by the administrators in line with their role.

Existing images can be used or new images can be added in line with branded look and feel. Landing pages can also be copied via the Clone option so they can be edited or exported and re-imported.

For designers with access to the tag function, this enables the landing page to be uniquely identified and a tag version can be applied to track and control changes.

The CSS of the Theme can be used to control the layout of the landing page.

### Create a Landing Page

#### Before You Begin

To work on an existing Landing Page, it is recommended to clone it and work on the clone.
Procedure

Step 1  Login as the provider admin.
Step 2  Choose the hierarchy for the Landing Page.
Step 3  From the left menu, select **Role Management > Landing Pages**.
Step 4  Click **Add**.
Step 5  On the **Base** tab, enter a name for the Landing page.
Step 6  Click the + button on the **Meta Tasks** field and fill in the necessary information.
Step 7  Click the + button on the **Sections** field and fill in the necessary information.
Step 8  On the **Welcome Header** tab, enter the required Header Text, which is a single line static welcome message displayed on top of the Landing page.
Step 9  Enter the required Line Text, for the welcome line displayed under the header.
Step 10 Click Add adjacent to links, for each required link in the section, and enter the link details. The available fields are for menu items when creating Menu Layouts. If Type is selected, field display policies and configuration templates can be applied. The link Type is displayed as the chosen Display As item:

- Form - Show an input form (for an Href value, a resource ends with "/add/").
- List - List view of a resource referenced by Type or Href.
- Tree - A tree view of resource to display (if the system Href provides a tree path).
- Wizard - Execute a wizard referenced by the Href. The wizard resource URL ends with "/0/".
- IFrame - A URL specified as the Href value opens as an IFrame for cross-launching.

Step 11 Arrange the desired order of the sections by clicking the up or down arrows to move the sections up or down respectively.
Step 12 Click **Save**.

**What to Do Next**
Assign the Landing Page to the appropriate Roles.

### Landing Page Field Reference

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header Text *</td>
<td>header</td>
<td>A single line static welcome test displayed on top of the landing page.</td>
</tr>
<tr>
<td>Line Text *</td>
<td>line</td>
<td>Text for the welcome line displayed under the header. Use [userrole] as a placeholder to insert the current user's role.</td>
</tr>
</tbody>
</table>
### Meta Tasks

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meta Tasks</td>
<td>meta_tasks</td>
<td>Definitions for the meta task shortcut buttons</td>
</tr>
</tbody>
</table>

### Base

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meta Tasks</td>
<td>meta_tasks</td>
<td>Definitions for the meta task short-cut buttons.</td>
</tr>
<tr>
<td>Sections</td>
<td>sections</td>
<td>The list of section items that belong to the Landing Page.</td>
</tr>
</tbody>
</table>

### Meta Tasks

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display As</td>
<td>display</td>
<td>Select the display format of the model types of the menu item. The format can be a Form for a single instance, or a Tree or List for more than one instance.</td>
</tr>
<tr>
<td>Button Text</td>
<td>button_text</td>
<td>Text for the button</td>
</tr>
<tr>
<td>Type</td>
<td>type</td>
<td>The selected model type from the Type drop-down list to associate with the Title.</td>
</tr>
<tr>
<td>Href</td>
<td>href</td>
<td>If a direct reference to a model type is used for the menu item, the specified path.</td>
</tr>
<tr>
<td>Field Display Policy</td>
<td>field_display_policy</td>
<td>The selected Field Display Policy that is associated with the Menu Item.</td>
</tr>
<tr>
<td>Configuration Template</td>
<td>configuration_template</td>
<td>The selected Configuration Template that is associated with the Menu Item.</td>
</tr>
</tbody>
</table>

### Sections

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title *</td>
<td>title</td>
<td>The section title as it will show on the Landing page.</td>
</tr>
<tr>
<td>Image URL</td>
<td>image</td>
<td>Optional URL to image to be displayed as section image.</td>
</tr>
<tr>
<td>Links</td>
<td>links</td>
<td>List of links that belong to section.</td>
</tr>
</tbody>
</table>
Links

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display As</td>
<td>display</td>
<td>Select the display format of the model types of the menu item. The format can be a Form for a single instance, or a Tree or List for more than one instance.</td>
</tr>
<tr>
<td>Display Multiple Columns</td>
<td>is_multicolumn</td>
<td>Determines if link is shown as multiple columns or not</td>
</tr>
<tr>
<td>Link Text</td>
<td>link_text</td>
<td>Text for the link</td>
</tr>
<tr>
<td>Columns</td>
<td>columns</td>
<td>Determines if links are shown as single or multiple columns</td>
</tr>
<tr>
<td>Type</td>
<td>type</td>
<td>The selected model type from the Type drop-down list to associate with the Title.</td>
</tr>
<tr>
<td>Href</td>
<td>href</td>
<td>If a direct reference to a model type is used for the menu item, the specified path.</td>
</tr>
<tr>
<td>Field Display Policy</td>
<td>field_display_policy</td>
<td>The selected Field Display Policy that is associated with the Menu Item.</td>
</tr>
<tr>
<td>Configuration Template</td>
<td>configuration_template</td>
<td>The selected Configuration Template that is associated with the Menu Item.</td>
</tr>
</tbody>
</table>

**Landing Page Definition**

The landing page definition comprises the following:

- **Name** - A landing page name.
- **Meta Tasks** - Allows you to add one or more shortcut buttons at the top of the home page screen (directly below the line text - if configured).
- **Sections** - One or more items displayed as a distinct block on the landing page. Sections are further broken down to:
  - **Title** - The heading given to the section.
  - **Image URL** - The image or icon that is displayed for a section. For example, if a theme was uploaded with landing page images and inside a sub folder of the theme folder is a file called `mytheme/img/landingpage/landing1.png`, then the URL would be: `/www/themes/mytheme/img/landingpage/landing1.png`.
  - **links** - One or more links for a section, described in the table below.
Customizations

Landing Page Definition

Also refer to data/LandingPage on-line help.

<table>
<thead>
<tr>
<th>Meta Tasks / Links Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display As</td>
<td>Determines how the link is displayed. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Form - The link opens using a form widget.</td>
</tr>
<tr>
<td></td>
<td>• Inline List - The link points to the first five list of items.</td>
</tr>
<tr>
<td></td>
<td>• List - Link target is rendered using the list widget.</td>
</tr>
<tr>
<td></td>
<td>• Tree - Display the link target using a tree widget.</td>
</tr>
<tr>
<td></td>
<td>• Wizard - Display the link target as a wizard.</td>
</tr>
<tr>
<td></td>
<td>• IFrame - Display the link target in an iFrame. Used for x-launch.</td>
</tr>
<tr>
<td></td>
<td>If the Inline List option is chosen, the Display Multiple Columns field is visible. The first five items are displayed in the section. If the list is longer than five items, a link to the whole list is displayed after the first five.</td>
</tr>
</tbody>
</table>

| Display Multiple Columns | If Display As is set to Inline List, the check box determines if the single field or multiple fields are to be shown. If enabled, the Link Test field is hidden and replaced by the Columns field. |

| Button Text (Meta Tasks section only) | Text that is displayed in the task's button. |
| Link Text (Links section only)       | Text that is displayed in the link's button. |
| Columns                               | The names of the columns to be displayed from the list of fields returned by the API. This field is mutually exclusive with Columns. The fields are displayed as links to the target list items. For example, if `first_name` and `last_name` are selected for `data\User`, then the first five users are listed as rows with columns for the first name and last name. |
| Type                                  | The Model Type that is displayed or targeted by the link. If this field is populated, then the Href field (below) should be blank. For example, if `Model Type` is selected as `data/User` and the `Display As` option is `List`, then the menu link shows the list of instances of `data/User`. |
| Href                                  | API URL on which the client performs retrieves the link's data from If this field is populated, then the Type field (above) should be blank. An example API URL would be `/api/v0/relation/SubscriberPhone/` for a list of items of type relation/SubscriberPhone. |
Field Display Policies

Field Display Policies are applied to certain item types in order to modify the default form that is displayed when these items are created or accessed.

With Field Display Policies, the fields on an item detail form can be grouped, hidden; on-line help text can be added and a field can be set as read-only. A field can be provided with a new label and its order on the form can be re-sequenced. The order parameter is the relative position in the group.

More than one Field Display Policy can apply to a particular item type so that the selection of a particular policy will present another view of the form.

A Field Display Policy for an item type can be applied from a Menu Layout by selecting and associating it with the item on the Menu Layout. The Menu Layout is then selected to be part of a user Role so that users who have this role and log in will be able to have the item displayed according to the relevant Field Display Policy.

For example, a system may have users at Provider, Customer and Site administration hierarchy levels - all of whom may access the same items, but perhaps some item fields need to be hidden for administration users at a certain level. Field Display Policies can then be made that are applied to the Menu Layout associated with the administration users at these levels.

A quick way to carry out this task is to clone an existing Field Display Policy, modify it as required and then to select it for the model on a user's menu layout. In this way a user's interface can be modified from the point of user access to the model on the menu.

There is a unique constraint on the name of the clone per hierarchy level, so the same name as the original can be used on another hierarchy, but a new name is needed at the same hierarchy.

<table>
<thead>
<tr>
<th>Meta Tasks / Links Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Display Policy</td>
<td>If specified, the Form URI is extended to apply the policy to the returned form. For example, if <strong>Model Type</strong> is selected as <code>data/User/add</code> and <strong>Display As</strong> option is <strong>Form</strong>, then a Field Display Policy that is available for <code>data/User</code> can be selected to apply to the form in order to for example hide or rename input fields.</td>
</tr>
<tr>
<td>Configuration Template</td>
<td>If specified, the Form URI is extended to apply the template to the returned form. For example, if <strong>Model Type</strong> is selected as <code>data/User/add</code> and <strong>Display As</strong> option is <strong>Form</strong>, then a Configuration Template that is available for <code>data/User</code> can be selected to apply to the form in order to, for example, provide default values.</td>
</tr>
<tr>
<td>Link Text</td>
<td>The text that is displayed as the link. If the link is displayed as Inline Form, then a field name from returned data type may be specified instead. This field is mutually exclusive with Columns. Note that if the display is Inline List, then all displayed links show this text.</td>
</tr>
</tbody>
</table>
A Field Display Policy can also be selected for a form that is part of a Wizard. If a Field Display Policy is called 'default', it will apply to a model by default.

Clone a Field Display Policy

Procedure

1. Login as hcsadmin or provider administrator.
2. Choose the desired hierarchy.
3. From the left menu, select Role Management > Field Display Policies.
4. Click on the Field Display Policy that you want to clone.
5. Click the Actions button and choose Clone.
6. Update the necessary fields for the cloned Field Display Policy.
7. Click the Save button.

Field Display Policy Field Reference

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name *</td>
<td>name</td>
<td>The name that is given to the Field Display Policy.</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td>A description for the Field Display Policy instance.</td>
</tr>
<tr>
<td>Target Model Type *</td>
<td>target_model_type</td>
<td>The target model type to which the Field Display Policy applies.</td>
</tr>
<tr>
<td>Groups</td>
<td>groups.[n]</td>
<td>The groups that describe groupings of attributes that are displayed together on the user interface.</td>
</tr>
<tr>
<td>Title *</td>
<td>title</td>
<td>The name of a specific group of attributes.</td>
</tr>
<tr>
<td>Display as Fieldset</td>
<td>display_as_fieldset</td>
<td>Render this group as a fieldset in the form.</td>
</tr>
<tr>
<td>Number of Columns</td>
<td>num_cols</td>
<td>The number of columns of fields.</td>
</tr>
<tr>
<td>Policy *</td>
<td>policy</td>
<td>The specific policy application to attributes of the target model type of the Field Display Policy.</td>
</tr>
</tbody>
</table>
Configuration Templates

Configuration templates are used to define values for attributes of any model. The values can be fixed values or existing macros visible from the hierarchy context where the configuration template is applied. The templates provide a useful way to define default values for items that are exposed in the GUI (visible, invisible or read only). They also provide a mechanism to map data from data input via the GUI or device model events to other models or Provisioning Workflows in the system.

One may want to hide attributes of a model whilst setting them to a specific fixed value (e.g. a hardcoded setting); or one may wish to derive the value based on a macro (for example, look up the value based on data in the system).

For example, if a model has an attribute that is defined to be a date string, a Configuration Template for the attribute can be defined as a macro `{{fn.now "$Y-$m-$d"}}` in order to set the current date stamp as the value, such as `2013-04-18`. Designers can access reference material for details on macros.

Another example is a model such as the Quick Add Subscriber that limits the user input to a few fields, whilst deriving the value of other hidden attributes from various Configuration Templates that are each applied to different underlying models that make up a Subscriber (for example, Voicemail account settings, conference account settings, phone, line, device profile settings, and so on).

When an instance of the model is added or updated, the Configuration Template that has been enabled for the model applies. For array elements of data- and domain models, a list and a variable can be specified to be looped through so that a value is applied to each element in the model array.

More than one Configuration Template can be created for a model. These can then be used as needed. Configuration Templates can also be applied to models in the design of for example Provisioning Workflows and Wizards.

A Menu Layout that can be associated with a user role can also apply a Configuration Template to a model that is selected as a menu item.

For administrators at Provider Administrator level of higher, a quick way to create a Configuration Template would be to open a similar template from for example the Role Management > Configuration Templates menu and to customize a clone of it.

Administrators at levels above the Site Administrator can also customize these templates, including Field Display Policies.
Clone a Configuration Template

Procedure

Step 1  Login as hcsadmin or provider administrator.
Step 2  Choose the desired hierarchy.
Step 3  From the left menu, select Role Management > Configuration Templates.
Step 4  Click on the Configuration Template that you want to clone.
Step 5  Click the Actions button and choose Clone.
Step 6  Update the necessary fields for the cloned Configuration Template.
Step 7  Click the Save button.

Configuration Template Field Reference

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name *</td>
<td>name</td>
<td>The name that is given to the Configuration Template.</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td>A description for the Configuration Template instance.</td>
</tr>
<tr>
<td>Foreach Elements</td>
<td>foreach.[n]</td>
<td>Iterates over the list returned by the macro and appends array elements to the specified field.</td>
</tr>
<tr>
<td>Property *</td>
<td>property</td>
<td>The field/property to iterate over.</td>
</tr>
<tr>
<td>Macro List *</td>
<td>macro_list</td>
<td>The macro that produces the list to iterate over.</td>
</tr>
<tr>
<td>Context Variable *</td>
<td>context_var</td>
<td>The context variable that will contain the data from the iteration.</td>
</tr>
<tr>
<td>Target Model Type *</td>
<td>target_model_type</td>
<td>The target model type and name that the Configuration Template applies to.</td>
</tr>
<tr>
<td>Template *</td>
<td>template</td>
<td>The contents of the template, such as defaults and macros. The names shown in the template are determined by the attribute names of the Target Model Type.</td>
</tr>
</tbody>
</table>
Access Profiles

Access profiles define model types that a user is permitted to access. Access profiles are assigned to users via Roles.

Clone an Access Profile

**Procedure**

**Step 1**  
Login as hcsadmin.

**Step 2**  
From the left menu, select **Role Management > Access Profiles**.

**Step 3**  
Click on the Access Profile you want to clone.

**Step 4**  
Click the **Actions** button and choose **Clone**.

**Step 5**  
Enter the name, description and assign the necessary permissions for the Access Profile you are creating.

**Step 6**  
Click the **Save** button.

Access Profile Field Reference

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name *</td>
<td>name</td>
<td>The name that is given to the Access Profile.</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td>A description for the Access Profile.</td>
</tr>
<tr>
<td>Full Access</td>
<td>full_access</td>
<td>Enabling this flag, grants the user full system access.</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>miscellaneous_permissions</td>
<td>The list of miscellaneous operations permitted by this Access Profile.</td>
</tr>
<tr>
<td>Permissions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type Specific</td>
<td>type_specific_permissions</td>
<td>The list of types that are permitted by this Access Profile.</td>
</tr>
<tr>
<td>Permissions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Type Specific Permissions**

<table>
<thead>
<tr>
<th>Title</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permitted Type</td>
<td>type</td>
<td>The type that is permitted by this Access Profile. This field supports the use of the * wildcard.</td>
</tr>
<tr>
<td>Title</td>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Permitted Operations</td>
<td>operations</td>
<td>The operations that are permitted by this Access Profile for the given type.</td>
</tr>
</tbody>
</table>
Bulk Loading

• Bulk Loading a File, page 253

Bulk Loading a File

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Login to the necessary hierarchy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the left menu, choose Administration Tools &gt; Bulk Load menu.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Browse button and choose the required file and select Open.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Bulk Load File.</td>
</tr>
</tbody>
</table>
CHAPTER 17

Backup and Restore

• Backups, page 255

Backups

Backups represent a snapshot of the system, including database, configuration and system applications. Backups can be created manually, scheduled automatically, or created automatically when the system is upgraded. These backups can be stored on the local file system, or to a remote network location. There is no direct requirement for Vmware snapshots. For examples of backup maintenance commands and output, refer to the topics on Scheduling and Create a Backup.

If the Cisco Unified Communications Domain Manager 10.6(1) node is not recoverable, due to for example a hardware failure, a new node can be deployed and an existing backup restored to restore the node to service.

Backup Destinations

Backups can be made to the local file system or a remote destination.

• Display available backup destinations with backup list.
• Add a new backup destination with backup add <location-name> <URL>.

Local backups are stored on a separate backup volume and the localbackups destination is pre-configured. If the backup volume is too small, it can be increased in size.

Note

If the localbackups destination is removed or renamed, an ISO file upgrade will no longer function. Therefore, it is imperative that this destination is not removed.

Example:

backup add myserverbackup sftp://user@server/path

Backups to sftp require ssh key-based authentication to be setup.

If a common remote backup point is to be used by all nodes in the cluster, the backup destination needs to be added to each node. This can be automated by using cluster remote execution, for example:
cluster run all backup add myserverbackup sftp://user@server/path

Create Space for a Backup or Restore

If a No space left on device message is received during a backup or a restore, carry out the following steps:

Procedure

Step 1 In VMware, add a disk to the system:
   a) Click on VM > Edit Settings.
   b) Click Add.
   c) Select Hard Disk, then Create a new virtual disk.
   d) Set the size to be the same as the DB disk - 250GB.
   e) Click Finish

Step 2 Log into platform account, and run drives list. Make note of the disk under Unused disks:.

Step 3 Run drives reassign <disk from step 2> services:backups.
   Once done, all current data would have been moved to new disk and the old one can be removed from VMware. The restore command can now be rerun.

Adding More Space to Accommodate a Large Restore

Procedure

Step 1 Right click on the VM in the Vmware Client and click Edit Settings.

Step 2 On the Hardware tab, click Add.

Step 3 Follow the wizard to add a new hard disk to the VM with the correct size.

Step 4 If the restore size exceeds both the backup and dbroot drives size, ensure you add two hard disks to the VM. In a clustered environment, this procedure needs to be performed on all of the DB nodes.

Backup Passphrase

System backups are encrypted. The encryption key is initially set as the platform user's password as set in the installation wizard. It is recommended that this be changed after installation. This can be done by running backup passphrase.

The following example shows the console output:

platform@masternode:~$ backup passphrase
Please enter current backup passphrase
Password:
Please enter new backup passphrase
Password:
Please re-enter new backup passphrase
Password:
Backup passphrase successfully changed
This password needs to be kept, because restoring the backup to a new system will require this password to be the same as above.
To restore on the new system, run the above command and enter password used to create the backup

Setting up the Backup Passphrase on a New Environment

To set the backup passphrase to restore on a different environment:

Procedure

| Step 1 | Log into the new environment. If this is a cluster deployment, log in on the DB Primary. |
| Step 2 | Run the `backup passphrase` command. |
| Step 3 | Specify the current passphrase. This is normally the password of the platform user set during the deploy of the system. |
| Step 4 | Enter the new passphrase twice. |

Reassign Current Drives (Backup and DBroot)

Procedure

| Step 1 | Once the hard disks are added, reassign the drives using the `drives reassign <disk> <mountpoint name>` command. |
| Step 2 | Use the `drives list` command to list the new drives added through VMware. For example, if the new drive is listed as `sdf`, use the reassign command as follows: `drives reassign sdf services:backups`. |
| Step 3 | Similarly, to reassign the dbroot, use the reassign command as follows: `drives reassign sde mongodb:dbroot`. |

Create a Backup

Backups can be created using `backup create <destination>`, for example:

`backup create localbackups` or `backup create myserverbackup <remote destination>`.

An example of the console output is shown below:

```
platform@myhost:~$ backup create localbackup
... collecting data
... preparing mongo data backup
... Backing up database <name>
```
Backup and Restore

.. Backing up database <name>_FILES
.. Backing up database <name>_EXPORT
... Not backing up database local
... Backing up database PLATFORM
......................
... Backing up database admin
.
... creating backup
98% completed
... verifying backup
Backup was successfully created at file:///backups/a0b26a1a267a1582e2aa0258a4fa85b75d4b09bb
WARNING: Backup maintenance of this location is not scheduled
schedule add localbackup-maintain backup clean localbackup keep 5
platform@myhost:~$ backup list localbackup
localbackup:
  URI: file:///backups
  Backups:
    2014-06-18 16:26
Backups contain all application data.
Backups can be scheduled to run automatically - refer to the schedule command to automated backups.
For example:

  • schedule add mybackups backup create myserverbackup
  • schedule time mybackups 2 0
  • schedule enable mybackups

The cluster-wide backup can be created using the command cluster run all backup create myserverbackup after creating the destination with for example cluster run all backup add myserverbackup sftp://user@server/path. Generally, it is not recommended that a cluster wide backup be scheduled from a single node, since failure of the scheduled node could result in missing backups. Rather schedule a backup per node as above.

If a common network URI is used as backup destination across the cluster, each node's backup will be uniquely identified by its UID in the remote backup directory.

Restore the Backup

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Copy the backup to the environment with scp. It will be located in the media/ folder.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Once the file is successfully copied, use the backup import command to import the backup to a location that was set up, or the default localbackup.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Once the import is complete, run the backup list command as for example: platform@Restorer:~$ backup list localbackup:</td>
</tr>
</tbody>
</table>
**URI:** file://backups
**Backups:**
1 backups have been created - most recently 2015-02-26 00:22

**Step 4** Run the `backup restore` command as for example:
platform@Restore:~$ backup restore localbackup 2015-02-26 00:22

---

**Restore a Backup in a Clustered Environment**

In a clustered environment, servers can allow for failures and keep data intact, because when a server fails, an automatic failover occurs. If all services are kept running and data remains accessible, a backup restore would only be necessary in very specific scenarios.

Restoring a backup in a cluster would only be necessary in the following cases:

- Data Corruption (Bad Data)
- Losing the whole cluster - requiring a redeploy of new servers

---

**Example of a Successful Restore**

platform@Restore:~$ backup restore localbackup 2015-02-26 00:22
Services will be restarted during the restore. Do you wish to continue? y
Application voss-deviceapi processes stopped.
Stopping Application while performing database restore

--- Restore, ip=172.29.41.240, role=webproxy,application,database, loc=jhb

Application nginx processes stopped.
System restore starting from file:///backups/93d19980b574ed743d9b000a7595e42cad6a6d6b
(1424910132)
Local and Remote metadata are synchronized, no sync needed. Last full backup date: Thu Feb 26
00:22:12 2015
Successfully restored to /backups/appdata/restore_temp_1427441507, moving to /backups/appdata
Removing temporary files in /backups/appdata/restore_temp_1427441507 local\|admin
Dropping database PLATFORM before restoring MongoDB shell version: 2.6.1
    connecting to: 127.0.0.1:27020/PLATFORM [object Object]
Repairing database PLATFORM before restoring MongoDB shell version: 2.6.1
    connecting to: 127.0.0.1:27020/PLATFORM [object Object]
Dropping database VOSS_FILES before restoring
    MongoDB shell version: 2.6.1
    connecting to: 127.0.0.1:27020/VOSS_FILES [object Object]
Repairing database VOSS_FILES before restoring MongoDB shell version: 2.6.1
    connecting to: 127.0.0.1:27020/VOSS_FILES [object Object]
Dropping database VOSS before restoring
    MongoDB shell version: 2.6.1
    connecting to: 127.0.0.1:27020/VOSS [object Object]
Repairing database VOSS before restoring MongoDB shell version: 2.6.1
    connecting to: 127.0.0.1:27020/VOSS [object Object]
Trying with oplogReplay restore successfull
    {"172.29.41.240": (200, "\n")}
Starting Application after performing database restore
--- Restore, ip=172.29.41.240, role=webproxy,application,database, loc=jhb
Application services:firewall processes stopped. Application nginx processes started.
Restarting services
Application processes stopped. Application processes started.
System settings have changed, please reboot using 'system reboot'
Restored successfully
You have new mail in /var/mail/platform
Maintaining Backups

A complete list of backups on a location can be displayed using `backup list <location>`.

Backups can be deleted using the following commands:

- `backup clean <location> keep <N>` will delete older copies so that only N copies are kept
- `backup clean <location> before <yyyy-mm-dd [HH:MM]>` will delete copies older than the specified date.

By default, there is no regular maintenance of backups, and a scheduled job should be created to perform this maintenance, for example:

- `schedule add backuprotate backup clean localbackups keep 5`
- `schedule time backuprotate rotate 3 0`
- `schedule enable backuprotate`

Exporting Backups

The backups are encrypted and may comprise of multiple files on the backup destination.

If a backup is to be exported to another system, it must be exported with the command:

`backup export <location> <destination-URI> <yyyy-mm-dd [HH:MM]>`

For example:

`backup export local backup destination-location 2014-04-30 11:16`

In turn, the backup can be imported on the remote server using `backup import <source-URI>`.

Scheduling

Any CLI command can be scheduled to run automatically, including but not restricted to backups and security upgrades.

By default there is no backup maintenance scheduled. Backup maintenance can be scheduled with the number of copies to be kept.

The automated job schedule format is as follows:

- `schedule add <job-name> <user-command>`
- `schedule time <job-name> <hour> <minute>`
- `schedule time <job-name> every <N> hours`
- Alternatively the job can be scheduled to run every week on Monday with `schedule time <job-name> weekly 1`; where 0 is Sunday, 1 is Monday, 2 is Tuesday, 3 is Wednesday, 4 is Thursday, 5 is Friday and 6 is Saturday
- `schedule enable <job-name>`

Example:
schedule add mybackups backup create localbackups
schedule time mybackups 2 0
schedule time mybackups weekly 0
schedule enable mybackups

Among the tasks that can be scheduled are:

- Backup creation, e.g. `schedule add backupme backup create localbackup`
- Backup maintenance, e.g. `schedule add backupclean backup clean localbackup keep 5`
- Health reports, e.g. `schedule add reports diag report`

## DR Failover

The Cisco Unified Communications Domain Manager 10.6(1) system makes use of database replication facilities during normal operation. During a failover, if 50% or more of the service resources are lost, the system will no longer function without manual intervention. In this case, the following process should be followed.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Display the current cluster topology using <code>cluster status</code>.</th>
</tr>
</thead>
</table>
| Step 2 | Remove the dead nodes using `cluster del <ip>`.
| Step 3 | Once the cluster topology is adjusted, the cluster must be reprovisioned using `cluster provision`.
| Step 4 | Afterward, the cluster status can be rechecked with `cluster status`. |

## DR Failover and Recovery

### DR Failover and Recovery Scenarios

A number of failover scenarios and recovery steps are shown. In each case, a node topology is assumed, a node failure scenario is indicated and a set of recovery steps are provided.

Cisco Unified Communications Domain Manager System Recovery is supported from the following failover scenarios:

- Loss of a non-primary node in the Primary site
- Loss of a non-primary server in the DR site
- Loss of the Primary Database Server
- Loss of a Primary Site
- Loss of a DR Site
For the scenarios below, the following procedures and definitions apply:

- In the event of a network failure or a temporary network outage affecting a single node, the node will be inaccessible and the cluster will respond in the same way as if the node had failed. If network connectivity is then restored, no action is required, because the node will again start communicating with the other nodes in the cluster, provided no changes were made to that node during the outage window.

- In a clustered deployment, the datacentre would typically be two different datacentres, for example “Virginia” and “Seattle”. These can be thought of as a primary site and a DR (Disaster Recovery) site in case of a failure in the primary site. These two datacentres can exist on the same physical hardware, so the separation of the cluster is into two sets of three nodes.

When datacentres are defined during installation, the nodes of a cluster may or may not be in the same physical location. The cluster is designed to communicate across all nodes, regardless of their physical location.

**Scenario: Loss of a Non-primary Node in the Primary Site**

- The administrator deployed the cluster into a Primary and DR site.

- The cluster is deployed according to the *Cisco Unified Communications Domain Manager Planning and Install Guide*.

- The example is a typical cluster deployment: 6 nodes, where 4 nodes are database servers and 2 nodes are proxy servers. The design is preferably split over 2 physical data centers.

```
Data Centre: jhb
  application : AS01[172.29.42.100]
                AS02[172.29.42.101]
  webproxy :   PS01[172.29.42.102]
                AS01[172.29.42.100]
                AS02[172.29.42.101]
  database :   AS01[172.29.42.100]
                AS02[172.29.42.101]

Data Centre: cpt
  application : AS03[172.29.21.100]
                AS04[172.29.21.101]
  webproxy :   PS02[172.29.21.102]
                AS03[172.29.21.100]
                AS04[172.29.21.101]
  database :   AS03[172.29.21.100]
                AS04[172.29.21.101]
```

**Node Failure**

- Normal operations continue where the cluster is processing requests and transactions are committed successfully up to the point where a loss of a primary node is experienced. In this scenario AS02[172.29.42.101] failed while transactions were running.

- Examine the cluster status running **cluster status** to determine the failed state:

```
platform@AS01:~$ cluster status

  Data Centre: unknown
  application : unknown_172.29.42.101[172.29.42.101] (not responding)
```
webproxy : unknown_172.29.42.101[172.29.42.101] (not responding)
database : unknown_172.29.42.101[172.29.42.101] (not responding)

Data Centre: jhb
application : AS01[172.29.42.100]
webproxy : PS01[172.29.42.102]
        AS01[172.29.42.100]
database : AS01[172.29.42.100]

Data Centre: cpt
application : AS03[172.29.21.100]
        AS04[172.29.21.101]
webproxy : PS02[172.29.21.102]
        AS03[172.29.21.100]
        AS04[172.29.21.101]
database : AS03[172.29.21.100]
        AS04[172.29.21.101]

• At this point, all transactions that are currently in flight are lost and will not recover.
• The lost transactions have to be rerun.
• With the database server AS02 [172.29.42.101] still down, replaying the failed transactions are successful.

Recovery Steps if the server that is lost, is unrecoverable:

1 A new unified node needs to be deployed. Ensure the server name, IP information and datacentre name is the same as on the server that was lost.
2 Run cluster del 172.29.42.101, because this server no longer exists.
3 Delete all database weights (database weight del <ip>), for example database weight del 172.29.42.101 .
4 Run cluster provision before the new server is added.
5 Switch on the newly installed server.
6 If the node will be a unified, application or web proxy node, run cluster prepnode on it.
7 Run cluster add <ip> of the new unified server to add it to the existing cluster.
8 Add database weights so that the are weights distributed throughout the cluster (database weight add <ip> <weight>).
9 Run cluster provision to join the new unified node to the cluster communications.

Scenario: Loss of a Non-primary Server in the DR Site

• The administrator deployed the cluster into a Primary and DR site.
• The cluster is deployed according to the Cisco Unified Communications Domain Manager Planning and Install Guide.
• The example is a typical cluster deployment: 6 nodes, where 4 nodes are database servers and 2 nodes are proxy servers. The design is preferably split over 2 physical data centers.

Node Failure

• Normal operations continue where the cluster is processing requests and transactions are committed successfully up to the point where a loss of a primary node is experienced. In this scenario AS02[172.29.42.101] failed while transactions were running.

• Examine the cluster status running cluster status to determine the failed state:

```
Data Centre: unknown
  application : unknown_172.29.42.101[172.29.42.101] (not responding)
  webproxy : unknown_172.29.42.101[172.29.42.101] (not responding)
  database : unknown_172.29.42.101[172.29.42.101] (not responding)

Data Centre: jhb
  Application : AS01[172.29.42.100]
                AS02[172.29.42.101]
  webproxy : PS01[172.29.42.102]
             AS01[172.29.42.100]
             AS02[172.29.42.101]
  database : AS01[172.29.42.100]
             AS02[172.29.42.101]

Data Centre: cpt
  application : AS03[172.29.21.100]
  webproxy : PS02[172.29.21.102]
             AS03[172.29.21.100]
  database : AS03[172.29.21.100]
```

• At this point, all transactions that are currently in flight are lost and will not recover.

• The lost transactions have to be rerun.

• With the database server AS02[172.29.42.101] still down, replaying the failed transactions are successful.

Recovery Steps if the server that is lost, is unrecoverable:

1. A new unified node needs to be deployed. Ensure the server name, IP information and datacentre name is the same as on the server that was lost.

2. Run cluster del 172.29.42.101, because this server no longer exists.

3. Delete all database weights (database weight del <ip>), for example database weight del 172.29.42.101

4. Run cluster add <ip> before the new server is added.

5. Switch on the newly installed server.

6. If the node will be a unified, application or web proxy node, run cluster prepn ode on it.

7. Run cluster add <ip> of the new unified server to add it to the existing cluster.
Add database weights so that the weights are distributed throughout the cluster (`database weight add <ip> <weight>`).

Run `cluster provision` to join the new unified node to the cluster communications.

**Scenario: Loss of the Primary Database Server**

- The administrator deployed the cluster into a Primary and DR site.
- The cluster is deployed according to the *Cisco Unified Communications Domain Manager Planning and Install Guide*.
- The example is a typical cluster deployment: 6 nodes, where 4 nodes are database servers and 2 nodes are proxy servers. The design is preferably split over 2 physical data centers.

**Node Failure**

- Normal operations continue where the cluster is processing requests and transactions are committed successfully up to the point where a loss of a primary database server is experienced. In this scenario `AS01 [172.29.42.100]` failed while transactions were running.
- Examine the cluster status running `cluster status` to determine the failed state:

```
Data Centre: unknown
  application : unknown_172.29.42.100[172.29.42.100] (not responding)
  webproxy : unknown_172.29.42.100[172.29.42.100] (not responding)
  database : unknown_172.29.42.100[172.29.42.100] (not responding)

Data Centre: jhb
  application : AS02[172.29.42.101]
  webproxy : PS01[172.29.42.102]
             AS02[172.29.42.101]
  database : AS02[172.29.42.101]

Data Centre: cpt
  application : AS03[172.29.21.100]
             AS04[172.29.21.101]
  webproxy : PS02[172.29.21.102]
             AS03[172.29.21.100]
             AS04[172.29.21.101]
  database : AS03[172.29.21.100]
             AS04[172.29.21.101]
```

- The loss of the Primary database server will cause an election and the node with the highest weighting still running will become primary. The election itself may take 10-30 seconds.
- Check the weights set in the cluster configuration: `database weight list`

```
platform@AS01:~$ database weight list
  172.29.21.100:
      weight: 10
  172.29.21.101:
      weight: 10
  172.29.42.100:
      weight: 20
```
172.29.42.101:
weight: 40

- The primary node 172.29.42.100 failed and therefore node 172.29.42.101 will become the primary node after election.
- To find the primary database, run `database primary`.

```
platform@AS02:$ database primary
172.29.42.101
```

- At this point all transactions that are currently in flight are lost and will not recover.
- The lost transactions have to be rerun.
- With the database server AS01 [172.29.42.100] still down, replaying the failed transactions is successful.

Recovery Steps if the server that is lost, is unrecoverable:
1. A new unified node needs to be deployed. Ensure the server name, IP information and datacentre name is the same as on the server that was lost.
2. Run `cluster del 172.29.42.100`, because this server no longer exists.
3. Delete all database weights (`database weight del <ip>`), for example `database weight del 172.29.42.101`
4. Run `cluster provision` before the new server is added.
5. Switch on the newly installed server.
6. If the node will be a unified, application or web proxy node, run `cluster prepnode` on it.
7. Run `cluster add <ip>` of the new unified server to add it to the existing cluster.
8. Add database weights so that the weights are distributed throughout the cluster (`database weight add <ip> <weight>`).
9. Run `cluster provision` to join the new unified node to the cluster communications.

**Scenario: Loss of a Primary Site**

- The administrator deployed the cluster into a Primary and DR site.
- The cluster is deployed according to the *Cisco Unified Communications Domain Manager Planning and Install Guide*.
- The example is a typical cluster deployment: 6 nodes, where 4 nodes are database servers and 2 nodes are proxy servers. The design is preferably split over 2 physical data centers.
- The cluster might also be in two geographically dispersed areas. The cluster has to be installed in two different site names or data center names. In this scenario, a portion of the cluster is in Johannesburg and the other is in Cape Town, South Africa:

```
Data Centre: jhb
  application : AS02[172.29.42.101]
  webproxy : PS01[172.29.42.102] AS02[172.29.42.101]
  database : AS02[172.29.42.101]
```

```
platform@AS02:$ database primary
172.29.42.101
```

- At this point all transactions that are currently in flight are lost and will not recover.
- The lost transactions have to be rerun.
- With the database server AS01 [172.29.42.100] still down, replaying the failed transactions is successful.

Recovery Steps if the server that is lost, is unrecoverable:
1. A new unified node needs to be deployed. Ensure the server name, IP information and datacentre name is the same as on the server that was lost.
2. Run `cluster del 172.29.42.100`, because this server no longer exists.
3. Delete all database weights (`database weight del <ip>`), for example `database weight del 172.29.42.101`
4. Run `cluster provision` before the new server is added.
5. Switch on the newly installed server.
6. If the node will be a unified, application or web proxy node, run `cluster prepnode` on it.
7. Run `cluster add <ip>` of the new unified server to add it to the existing cluster.
8. Add database weights so that the weights are distributed throughout the cluster (`database weight add <ip> <weight>`).
9. Run `cluster provision` to join the new unified node to the cluster communications.

**Scenario: Loss of a Primary Site**

- The administrator deployed the cluster into a Primary and DR site.
- The cluster is deployed according to the *Cisco Unified Communications Domain Manager Planning and Install Guide*.
- The example is a typical cluster deployment: 6 nodes, where 4 nodes are database servers and 2 nodes are proxy servers. The design is preferably split over 2 physical data centers.
- The cluster might also be in two geographically dispersed areas. The cluster has to be installed in two different site names or data center names. In this scenario, a portion of the cluster is in Johannesburg and the other is in Cape Town, South Africa:
Primary site failure

- Normal operations continue where the cluster is processing requests and transactions are committed successfully up to the point where a loss of a Primary site is experienced. In this scenario, AS01[172.29.42.100], AS01[172.29.42.101] and AS01[172.29.42.100] failed while transactions were running.

- At this point, all transactions that are currently in flight are lost and will not recover.

- Examine the cluster status by running `cluster status` to determine the failed state:

Data Centre: unknown
application : unknown_172.29.42.100 [172.29.42.100] (not responding)
unknown_172.29.42.101 [172.29.42.101] (not responding)
webproxy : unknown_172.29.42.100 [172.29.42.100] (not responding)
unknown_172.29.42.101 [172.29.42.101] (not responding)
unknown_172.29.42.102 [172.29.42.102] (not responding)
database : unknown_172.29.42.100 [172.29.42.100] (not responding)
unknown_172.29.42.101 [172.29.42.101] (not responding)

Data Centre: jhb
application :

webproxy :

database :

Data Centre: cpt
application : AS03[172.29.21.100]
AS04[172.29.21.101]
webproxy : PS02[172.29.21.102]
AS03[172.29.21.100]
AS04[172.29.21.101]
database : AS03[172.29.21.100]
AS04[172.29.21.101]

- The cluster will be not be operational and manual intervention is needed to recover if a continued flow of transactions is required with a minimum of downtime.

- To recover the lost nodes and if they are unrecoverable, carry out the following recovery steps.

Recovery Steps:

1. Run `cluster del <ip>` on the failed nodes from the existing half of the cluster.
2. Remove all database weights from the cluster: `database weight del <ip>`
At this point you do have the option to provision half the cluster for a faster uptime of your DR site. Only the DR site will be operational after the provision.

If you choose to bring the full cluster back up, you need to redeploy the primary site nodes if the nodes are unrecoverable without a doubt.

Run `cluster provision` before the new servers are added.

Deploy 3 nodes: 2 as unified nodes and 1 as a proxy node.

If the node will be a unified, application or web proxy node, run `cluster prepnode` on it.

After the redeployment, at this stage run `cluster add <ip>` for the nodes to become part of the cluster.

Add the database weights back, using `database weight add <ip> <weight>`

Run `cluster provision primary` to ensure that a primary is selected for the provisioning stage.

**Scenario: Loss of a DR Site**

- The administrator deployed the cluster into a Primary and DR site.
- The cluster is deployed according to the *Cisco Unified Communications Domain Manager Planning and Install Guide*.
- The example is a typical cluster deployment: 6 nodes, where 4 nodes are database servers and 2 nodes are proxy servers. The design is preferably split over 2 physical data centers.
- The cluster might also be in two geographically dispersed areas. The cluster has to be installed in two different site names or data center names. In this scenario, a portion of the cluster is in Johannesburg and the other is in Cape Town, South Africa:

  **Data Centre: jhb**

  - application : AS02[172.29.42.101]
  - webproxy : PS01[172.29.42.102], AS02[172.29.42.101]
  - database : AS02[172.29.42.101]

  **Data Centre: cpt**

  - application : AS03[172.29.21.100], AS04[172.29.21.101]
  - webproxy : PS02[172.29.21.102], AS03[172.29.21.100], AS04[172.29.21.101]
  - database : AS03[172.29.21.100], AS04[172.29.21.101]

**DR site failure**

- Normal operations continue where the cluster is processing requests and transactions are committed successfully up to the point where a loss of a DR site is experienced. In this scenario, AS03[172.29.21.100], AS04[172.29.21.101] and PS02[172.29.21.100] failed while transactions were running.
- At this point, all transactions that are currently in flight are lost and will not recover. The lost transactions have to be rerun.
- With the DR site still down, replaying the failed transactions is successful
Examine the cluster status by running `cluster status` to determine the failed state:

Data Centre: unknown
application : unknown_172.29.21.100[172.29.21.100] (not responding)
unknown_172.29.21.101[172.29.21.101] (not responding)
webproxy : unknown_172.29.21.100[172.29.21.100] (not responding)
unknown_172.29.21.101[172.29.21.101] (not responding)
unknown_172.29.21.102[172.29.21.102] (not responding)
database : unknown_172.29.21.100[172.29.21.100] (not responding)
unknown_172.29.21.101[172.29.21.101] (not responding)

Data Centre: jhb
application : AS01[172.29.42.100]
AS02[172.29.42.101]
webproxy : PS01[172.29.42.102]
AS01[172.29.42.100]
AS02[172.29.42.101]
database : AS01[172.29.42.100]
AS02[172.29.42.101]

Data Centre: cpt
application :
webproxy :
database :

The cluster will be operational, but only on the Primary Site.

You need to recover the lost nodes and if they are unrecoverable. Follow the recovery steps below.

Recovery Steps
1. Run `cluster del <ip>` on the failed nodes from the existing half of the cluster.
2. Remove all database weights from the cluster: `database weight del <ip>`
3. Run `cluster provision` before a new server is added.
4. If you choose to bring the full cluster back up, you need to redeploy the DR site nodes if the nodes are unrecoverable.
5. Deploy 3 nodes: 2 as unified nodes and 1 as a proxy node.
6. If a node will be a unified, application or web proxy node, run `cluster prepnode` on it.
7. After the redeployment, at this stage run `cluster add <ip>` for the nodes to become part of the cluster.
8. Add the database weights back, using `database weight add <ip> <weight>`
9. Run `cluster provision primary` to ensure that a primary is selected for the provisioning stage.
High Availability Disaster Recovery

High Availability Overview

High Availability (HA) is an approach to IT system design and configuration that ensures Cisco Unified Communications Domain Manager is operational and accessible during a specified time frame. This is achieved using redundant hardware and resources. If there is a failure, an automatic failover will occur to the secondary database node.

Default High Availability Disaster Recovery Scenario

Cisco Unified Communications Domain Manager 10.6(1) supports using off-the-shelf VMware tools. High Availability is implemented using VMware HA clusters, with data accessed via a central storage facility (SAN). VMware monitors the primary server, and should it fail, another instance of the VM is automatically started on a different hardware instance. Since data is shared on the SAN, the new HA instance will have access to the full dataset.

Disaster Recovery is implemented by streaming data updates to a separate DR instance that remains powered on. If the primary server fails, the DR instance can take over operation. The switch-over to DR instance is scripted, but must be invoked manually.

During a HA failover, the HA instance assumes the primary IP address, and no reconfiguration of other UC elements is required. However, in the case of a DR failover, interaction with other UC elements should be considered:

- DNS can be used effectively to provide hostname abstraction of underlying IP addresses. In such a case, a DNS update will allow existing UC elements to seamlessly interact with the new DR instance.
- If DNS is not available, and the UC elements cannot be configured with the IP address of the DR instance, it is necessary for the DR instance to assume the primary IP address. In such a case, the DR and the primary IP addresses can be swapped using the CLI interface. Standard networking practices should be employed to ensure that the IP address is correctly routed, e.g. Stretched layer-2 vLAN, and ensuring that the Primary and DR instances are not operated with the same IP address.

The following failure points should be considered:

- Since the HA instance is started automatically if the primary instance fails, a slight interruption in service is expected, including VMware polling latency in determining that the primary server has failed, and the startup delay of the HA instance. This delay is around 3 minutes.
- If data is corrupted on the SAN, the HA instance will start with the same corrupt code and data instances.
- Since VMware is checking only for VM liveness, it is not able to check that the primary instance is functionally active.
- Data updates are transported to the DR instance. If data updates cannot be shipped by the primary instance, SNMP traps are generated informing administration of the problem. However, if this is not fixed in a timely manner, it is possible for the DR instance to become out of sync. These delays could result in data loss between the primary and DR instances. Database updates are scheduled every 3 minutes and/or 16Mb.
**HA and DR Scenario with Cisco VMDC Geo-Redundancy Architecture**

High Availability and Disaster Recovery instances can be geo-relocated at will within the capabilities of the underlying network architecture.

For example, it is feasible to extend a VMware High Availability cluster geographically using high speed data links and layer-2 stretched vLANs.

Disaster Recovery as implemented by the Cisco Unified Communications Domain Manager 10.6(1) system lends itself to geographical separation with streaming data replication to a second powered-on instance.

Interaction with other UC elements must be considered within the capabilities of the network, using either DNS for seamless transition, or IP reconfiguration either within the UC elements or the Cisco Unified Communications Domain Manager 10.6(1) system.

**Configuring a HA System Platform on VMWare**

This is an optional step, however, for production servers it is highly recommended that they are run in a HA deployment configuration. This can be done by the client, but should be checked by a system representative.

**Procedure**

**Step 1** Log into VMware VSphere, then select **File > New >Cluster**.

**Step 2** Enter the Name, and select the Turn on VMware HA checkbox.

**Step 3** Make sure that the Enable Host Monitoring checkbox and Enable: Do not power on VMs that violate availability constraints radio buttons are selected.

**Step 4** Select the required default restart priority.

**Step 5** Select the VM Monitoring Only option from the VM Monitoring drop-down list, and set the Default Cluster Settings/Monitoring sensitivity to High.

**Step 6** Select the Disable EVC radio button, unless you know the exact version of CPU technologies that are enabled on your system.

**Step 7** Select the Store the swapfile in the same directory as the virtual machine (recommended) radio button.

**Step 8** Ensure the settings are all correct and click the **Finish** button.

**Step 9** Drag all of the machines that will be used into the newly created cluster.

**Step 10** Once done, they will be listed below the new cluster, with any VM’s that were moved into the root of the cluster.

**Step 11** Select each of the Machines in the cluster then select the Configuration tab.

**Step 12** If Time Configuration is displayed in red, select Properties, then click the **Options** button.

**Step 13** Select NTP Settings, and then click the **Add** button.

**Step 14** Select the Restart NTP service to apply changes checkbox, and then click the **OK** button.

**Step 15** Select the relevant Cluster, and then select the Summary tab. There should be no configuration issues listed.
Troubleshooting

'No Space Left on Device' Error

You receive the following error message while backing up or restoring Cisco Unified Communications Domain Manager 10.6(1) on a virtual machine: 'No Space Left on Device.' You can create a new virtual disk on the node with the primary database and then reassign the Cisco Unified Communications Domain Manager 10.6(1) data to the new disk. The new disk has enough space for you to perform the backup or restore operation.

Procedure

Step 1  Turn off the virtual machine that contains the primary database.
Step 2  In VMware, add a disk on the node that contains the primary database:
   a) From the VM menu, click Edit Settings.
   b) Click Add. The Add Hardware Wizard opens.
   c) Select Hard Disk and then click Next.
   d) Select Create a new virtual disk and then click Next.
   e) Set the capacity to be the same as the database disk: 250 GB.
   f) Accept the default file name and location, or click Browse to select a different location.
   g) Click Finish.
Step 3  Turn on the virtual machine. Your guest operating system recognizes the new virtual disk as a new, blank hard disk.
Step 4  Log in to the platform account on the virtual machine and run the drives list command.
Step 5  In the command output, note the following information, which you will use in step 6:
   • The name of the new disk in the 'Unused disks' section
   • The identifier of the current disk, 'services:backups,' in the 'Used disks and mountpoints' section
Step 6  Run the following command: drives reassign <new disk name> services:backups
All current data is moved to the new disk. You can continue with your backup or restore operation.

Loss of the whole cluster and redeploying new servers

The high level redeploy and backup restore steps are as follows:
   • Redeploy the cluster.
   • Store the backup you want to restore in a different location.
   • Recreate the remote backups on the primary node using backup create <loc-name> <URI>.
   • Copy the saved backup under the new UID folder on the remote backup server.
   • Do a backup list.
For example:

pxetest:
  URI: sftp://sftpusr:********@172.29.42.249/AS03
  Backups:
    1 backups have been created - most recently 2014-08-21 10:24

A backup restore can now be run on the primary.

The example console output below shows the steps and process:

Identifying the database primary:

platform@AS01:~$ database primary
172.29.42.100

Listing the backups:

platform@AS01:~$ backup list
localbackup:
  URI: file:///backups
  Backups:
    2 backups have been created - most recently 2014-08-21 17:59

pxetest:
  URI: sftp://sftpusr:********@172.29.42.249/AS01
  Backups:
    2 backups have been created - most recently 2014-08-21 12:54

You have new mail in /var/mail/platform

Restoring the backup:

platform@AS01:~$ backup restore pxetest 2014-08-21 12:54
Services will be restarted during the restore. Do you wish to continue? y

Stopping Application while performing database restore

------------ AS02, ip=172.29.42.101, role=webproxy,application,database, loc=cpt
Stopping nginx:proxy

------------ AS01, ip=172.29.42.100, role=webproxy,application,database, loc=cpt
Application nginx processes stopped.

------------ AS02, ip=172.29.42.101, role=webproxy,application,database, loc=cpt
Application nginx processes stopped.

------------ AS04, ip=172.29.21.191, role=webproxy,application,database, loc=jhb
Application nginx processes stopped.

------------ AS03, ip=172.29.21.190, role=webproxy,application,database, loc=jhb
Application nginx processes stopped.

System restore starting from
sftp://sftpusr:sftpusr@172.29.42.249/AS01/backupdata/restore_temp_1408699183
Local and Remote metadata are synchronized, no sync needed.
Last full backup date: Thu Aug 21 12:54:25 2014
Successfully restored to /backups/appdata/restore_temp_1408699183, moving to /backups/appdata
Removing temporary files in /backups/appdata/restore_temp_1408699183
local
Dropping database <name>_FILES before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/<name>_FILES
[object Object]
Repairing database `<name>_FILES` before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/<name>_FILES
[object Object]
Dropping database PLATFORM before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/PLATFORM
[object Object]
Repairing database PLATFORM before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/PLATFORM
[object Object]
Dropping database `<name>` before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/<name>
[object Object]
Repairing database `<name>` before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/<name>
[object Object]
Dropping database `<name>_LOCKING` before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/<name>_LOCKING
[object Object]
Repairing database `<name>_LOCKING` before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/<name>_LOCKING
[object Object]
Dropping database admin before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/admin
[object Object]
Repairing database admin before restoring
MongoDB shell version: 2.6.1
connecting to: 127.0.0.1:27020/admin
[object Object]
Trying with oplogReplay
Trying without oplogReplay
restore successful
Restarting services

Application processes stopped.

Application processes started.

System settings have changed, please reboot using 'system reboot'
System Maintenance

Use the platform user login application command line to perform maintenance - either by SSH or from the VM console command line. The password is configured during installation, and can be changed using `system password`. If the password is lost, it must be reset. To do this, please contact Support.

A local home directory is available to the user and can be managed by the user with standard Unix commands: `ls`, `cp`, `mv`, `rm`, `less`, `grep` and `scp`. The user is not permitted to view directories or run commands outside the home directory.

Typing `help` provides information on available commands. Entering the command without further parameters will provide additional information on that command. Refer to the output of the help command for more details.

The following brief command summary can be used to maintain the system.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>health</td>
<td>Provides a short system summary indicative of system health.</td>
</tr>
<tr>
<td>app status</td>
<td>Checks that all applications are running correctly.</td>
</tr>
<tr>
<td>app start</td>
<td>Restarts all services.</td>
</tr>
<tr>
<td>diag</td>
<td>Lists the available diagnostic commands.</td>
</tr>
<tr>
<td>network &lt;interface&gt; &lt;ip&gt; &lt;netmask&gt; &lt;gateway&gt;</td>
<td>Reconfigures the network interface, for example: <code>network eth0 192.168.1.2 255.255.255.0 192.168.2.1</code></td>
</tr>
<tr>
<td>system restart</td>
<td>Reboots the system.</td>
</tr>
<tr>
<td>system mount</td>
<td>Mounts any ISO images copied to the system so that the applications within it are visible.</td>
</tr>
</tbody>
</table>
### Cluster Failure Scenarios

The status of the cluster can be displayed from the command-line on any node using the command:

**cluster status**

The system can automatically signal email and/or SNMP events in the event that a node is found to be down. Refer to the diagrams in the section on deployments.

**Loss of an Application role**

The Web Proxy will keep directing traffic to alternate Application role servers. There is no downtime.

**Loss of a Web Proxy**

Communication via the lost Web Proxy will fail, unless some another loadbalancing infrastructure is in place (DNS, external loadbalancer, VIP technology). The node can be installed as a HA pair so that the VMware infrastructure will restore the node if it fails. Downtime takes place while updating the DNS entry or returning the Web Proxy to service. For continued service, traffic can be directed to an alternate Web Proxy or directly to an Application node if available. Traffic can be directed manually (i.e. network elements must be configured to forward traffic to the alternate Web Proxy).
Loss of a Database role

If the primary Database service is lost, the system will automatically revert to the secondary Database. The primary and secondary database nodes can be configured via the CLI using `database weight <ip> <weight>`. For example, the primary can be configured with a weight of 50, and the secondary with a weight of 20. If both the primary and the secondary Database servers are lost, the remaining Database servers will vote to elect a new primary Database server. There is downtime (usually no more than a few seconds) during election and failover, with a possible loss of data in transit (a single transaction). The GUI web-fronted transaction status can be queried to determine if any transactions failed. The downtime for a Primary to Secondary failover is significantly less and the risk of data loss likewise reduced. A full election (with higher downtime and risk) is therefore limited only to cases of severe outages where it is unavoidable. Although any values can be used, for 4 database nodes the weights: 4, 3, 2, 1 is recommended.

Loss of a site

Unified and Database nodes have database roles. The status of the roles can be displayed using `cluster status`. If 50% or more of the database roles are down, then there is insufficient availability for the cluster to function as is. Either additional role servers must be added, or the nodes with down roles must be removed from the cluster and the cluster needs to be reprovisioned. If there is insufficient (less than 50% means the system is down) Database role availability, manual intervention is required to reprovision the system – downtime is dependent on the size of the cluster. Refer to the Operations Guide for details on DR Failover. Database role availability can be increased by adding Database roles, providing greater probability of automatic failover. To delete a failed node and replace it with a new one if database primary is for example lost: The node can be deleted using `cluster del <ip>`. Additional nodes can be deployed and added to the cluster with `cluster add <ip>`. The database weights can be adjusted using `database weight <ip> <weight>`. Finally, the cluster can be reprovisioned with `cluster provision`.

The console output below shows examples of these commands.

The cluster status:
```
platform@cpt-bld2-cluster-01:~$ cluster status

Data Centre: jhb
 application : cpt-bld2-cluster-04[172.29.21.243]
               cpt-bld2-cluster-03[172.29.21.242]
 webproxy : cpt-bld2-cluster-06[172.29.21.245]
               cpt-bld2-cluster-04[172.29.21.243]
               cpt-bld2-cluster-03[172.29.21.242]
 database : cpt-bld2-cluster-04[172.29.21.243]
               cpt-bld2-cluster-03[172.29.21.242]

Data Centre: cpt
 application : cpt-bld2-cluster-02[172.29.21.241]
               cpt-bld2-cluster-01[172.29.21.240] (services down)
 webproxy : cpt-bld2-cluster-05[172.29.21.244]
               cpt-bld2-cluster-02[172.29.21.241]
               cpt-bld2-cluster-01[172.29.21.240] (services down)
 database : cpt-bld2-cluster-02[172.29.21.241]
               cpt-bld2-cluster-01[172.29.21.240] (services down)
```

Deleting a node:
```
platform@cpt-bld2-cluster-01:~$ cluster del 172.29.21.245
You are about to delete a host from the cluster. Do you wish to continue? y
```
Cluster successfully deleted node 172.29.21.245

Please run 'cluster provision' to reprovision the services in the cluster

Please note that the remote host may still be part of the database clustering and should either be shut down or reprovisioned as a single node BEFORE this cluster is reprovisioned.

You have new mail in /var/mail/platform

Adding a node:

platform@cpt-bld2-cluster-01:$ cluster add 172.29.21.245

Cluster successfully invited node 172.29.21.245

Please run 'cluster provision' to provision the services in the cluster

Database weights: listing and adding

platform@cpt-bld2-cluster-01:$ database weight list
  172.29.21.240:
    weight: 5
  172.29.21.241:
    weight: 3
  172.29.21.243:
    weight: 2
  172.29.21.244:
    weight: 1

platform@cpt-bld2-cluster-01:$ database weight 172.29.21.240 10
  172.29.21.240:
    weight: 10
  172.29.21.241:
    weight: 3
  172.29.21.243:
    weight: 2
  172.29.21.244:
    weight: 1
Networking

- Network Interfaces, page 279
- Network services, page 279
- Network URI specification, page 280

Network Interfaces

The command `network interfaces` will display the available network interfaces and their configuration. The hostname can be set or changed with `network name <hostname>`.

A network interface can be configured or changed as follows:

```
network <interface-name> <ip> <netmask> <gateway>
```

For example:

```
network eth0 172.29.89.100 255.255.255.0 172.29.89.44
```

The IP address can be changed without affecting the netmask and gateway using `network <interface-name> ip <ip>`, for example `network eth0 ip 172.29.89.100`.

The system should be rebooted after a network interface configuration or change. In the case of a standalone topology, the system should be provisioned again with the system provision command as the final step of the change.

Network routes can be displayed with `network routes`.

- A new network route can be configured with `network routes <subnet-name> <netmask> <gateway>`.
- Network routes can be deleted with `network route del <subnet-name>`.

Network services

Network security is described in detail under the Security section, including detail regarding firewall ports and so on.

NTP servers can be configured using the following commands:

- `network ntp` will display the configured NTP servers
• `network ntp add <ntp-server>` will add a NTP server
• `network ntp del <ntp-server>` will delete a NTP server

DNS servers can be configured using the following commands:
• `network dns` will display the configured DNS servers
• `network dns add <dns-server>` will add a DNS server
• `network dns del <dns-server>` will delete a DNS server
• `network domain <domain-name>` sets the default DNS domain
• Alternate DNS search domains can be configured with `network search add <domain>` and `network search del <domain>`

**Network URI specification**

All network locations are specified as a URI, for example download locations, backup destinations, notification destinations, and so on.

The following list shows the URI syntax:

• `ftp`: `ftp://user[:password]@host[:port][/path]`
• `http`: `http(s)://user[:password]@host[:port]/path`
• `file`: `file://[/path]+[/filename]`
• `sftp`: `sftp://user[:password]@host[:port][/path]`
• `scp`: `scp://[user@]host[:port]:[/path]`
• `Email`: `mailto:user@host`
• `snmpv2`: `snmp://community@host[:port]`
• `snmpv3`: `snmp://user:auth:password@host[:port] ... minimum auth/password`
Monitoring

- Application Control, page 281
- Notifications, page 283

Application Control

Application control

The functioning system is comprised of applications. Each application has a name and a version number. An application may have multiple processes running within and each process has its own state.

Application Status

The command app status is used to display the status of the system. When the command is executed, it requests an up-to-date status of every process, and hence may take a few seconds to return.

A typical app status screen from the command line interface:

```
platform@development:~$ app status
voss-deviceapi v1.1.1 (2014-08-20 17:16)
  |-voss-queue running
  |-voss-notifications running
  |-voss-wsgi running
template_creator v0.0.0
template_runner v0.0.0
mongodb v1.1.1 (2014-08-20 17:30)
  |-arbiter running
  |-database running
support v1.1.1 (2014-08-20 17:17)
  |  |-daemon running (completed)
  |  |-traps running (completed)
code v1.1.1 (2014-08-20 17:26)
platform v1.1.1 (2014-08-21 07:40)
nginx v1.1.1 (2014-08-20 17:27)
  |-proxy running
services v1.1.1 (2014-08-20 17:19)
  |-wsgi running
  |-logs running
  |-firewall running
```
The following states are defined:

- **running** indicates that the process is running correctly.
- **completed** indicates that the process ran to completion successfully.
- **suspended** indicates that the process is suspended while waiting for another process.
- **stopped** indicates that the process is not running. An error message indicates that the process stopped for an unexpected reason.

### Starting and Stopping

The system application may be stopped with `app stop` and restarted with `app start`. By default this is a non-blocking command, which means that the console prompt will be available after running this command while processes that are a part of it are running.

It is possible to start or stop individual applications and/or processes by appending the `<application-name>[:<process-name>]`. The list of applications can be seen by using the command `app status`.

For example, to stop the process `voss-queue`:

```
app start voss-queue
```

It is possible to perform a blocking start by including `blocking` after `start` but before the `<application-name>[:<process-name>]`. For example:

```
app start blocking
app start blocking voss-queue
```

This will ensure that all background processes that are started by `app start` will be completed before the console prompt is available.

### Remote Execution in Clusters

Commands can be run on a remote node and the output displayed locally using:

```
cluster run <nodename>|<role>|all
```

For example, `cluster run database app start mongodb` will restart the mongodb service on all database nodes.

`cluster run all backup create localbackup` will perform a local backup of each node on its local drive.

Sometimes there are long-running processes running on a server. To display such jobs, use the `cluster job list` command. It is also possible to re-attach to those jobs to see the output, using `cluster job reconnect <pid>`.

> Note
> When shutting down nodes in a cluster, this should be done individually on each node and not with the cluster run all command.
Notifications

Warnings and Notifications

On console login, the system displays a health report indicating the status of the system. This health report shows the following:

- Last login: Tue Sep 3 10:19:07 2013 from 172.29.232.68
- host: alan, role: standalone, load: 0.35, USERS: 3
- date: 2013-09-03 10:20:02 +00:00, up: 2:05
- network: 172.29.89.182, ntp: 172.29.1.15
- SECURITY_UPDATES: 136 security updates available
- database: 8.0Gb
- services: ok

The values in the report mean the following:

- last console login and IP address source
- the load average of the system
- the number of users currently logged in
- the system uptime
- the status of the system services
- whether security updates are available
- disk, CPU and memory warnings if applicable
- warnings are displayed in upper-case to draw attention

The report can be redisplayed by typing the command:

```
help
```

The system can be configured to forward warnings and notifications to a variety of destinations, including:

- local email
- remote email addresses
- remote SNMP destinations

Local email allows the administrator to view a list of warnings, and delete these as necessary.

SNMP queries

The server runs a SNMP server which can be queried remotely.

The following details identify the server:

- `snmp community <community string>`
- `snmp contact <system contact>`
- `snmp name <system name>`
• **snmp location <system location>**

SNMP CPU load notifications are set using:

```plaintext
snmp load <1min load> <5min load> <15min load>
```

which results in notifications being sent should the threshold be exceeded.

Incoming SNMP queries can be restricted to a single host for security purposes using:

```plaintext
snmp query <ip>
```

SNMP v2 can be set with:

```plaintext
snmp query snmp://<community string>@<ip>
```

SNMP v3 username and password can be set with:

```plaintext
snmp query snmp://user:auth:password@<ip>:<port>
```

Where:

- `user`: username for the SNMP3 trap server
- `auth`: the password (MD5 or SHA), with minimum length of 8 characters.
- `password`: the secondary password that is set for 'priv', with minimum length of 8 characters.

To verify what the version of snmp is currently in use, run `snmp list` and reference the `version` field.

The screen console output below is an example of the use of `snmp community <community string>`:

```bash
$ snmp list
  community: private7
  load1: 5
  load15: 3
  load5: 4
  query: snmp://private7@172.29.42.249
  syscontact: localhost
  syslocation: None
  sysname: None
  version: v2

$ snmp community private
  You are about to restart the SNMP service. Do you wish to continue? y
  Please update notify to reflect your latest changes.

$ snmp list
  community: private
  load1: 5
  load15: 3
  load5: 4
  query: snmp://private@172.29.42.249
  syscontact: localhost
  syslocation: None
  sysname: None
  version: v2
```
System Control

- System restart, page 285
- Passwords, page 285
- File Management, page 286
- Drive control, page 286

System restart

The system can be restarted with system reboot and shutdown with system shutdown.

Passwords

The password for the platform user is chosen at install time, but can be changed using system password which will then prompt for the old password, the new password and confirmation.

Passwords must contain:

- at least one upper case letter
- at least one lower case letter
- at least one number
- at least one symbol
- be at least 16 characters long

Additional users can be created with user add <username>. Refer to the System Security : Creating additional users section.

Each user can be granted access to specific commands offering role-based access control - Refer to System Security : Granting and revoking user rights.
File Management

Each user has a unique home directory in which local files can be stored. It is the user's responsibility to manage the disk space used by these files.

The command `disk diag` displays the disk usage. Files in the user's directory are displayed using the standard `ls` command, and deleted with `rm`.

New applications or upgrade packages are uploaded to the platform user using `scp` or `sftp`, for example `scp <filename> platform@192.168.0.1:` on the remote Unix file server.

A `sftp` or `scp` of files to Cisco Unified Communications Domain Manager 10.6(1) must be done in the media directory (`/opt/platform/admin/home/media`), which is a writable directory.

Alternatively a downloadable URL can be downloaded directly on the Cisco Unified Communications Domain Manager 10.6(1) system using `system download <URL>` and the downloaded file is placed in the platform user's directory. For example: `system download http://myserver/path/myfile.iso`

Individual applications are installed using `app install <filename>.script`. A list of available applications and versions is displayed using the command `app list`.

ISO packages include all the individual packages required for upgrading. Upgrade the system using `app upgrade <filename>.iso`. Alternatively, the ISO package file system can be mounted with the system `mount` command, and the individual applications are visible under the media directory, and visible via the `app list` command.

Drive control

In order to reduce the risk of `disk full` errors, the platform divides the file system over several disks keeping areas liable to grow outside the main root file system. The areas with the highest growth such as logs and database storage are kept on their own private file systems.

These disk mounts can be migrated onto new, larger disks and some other locations can optionally be moved onto their own disks. This is managed through the `drives` command.

The current mounted file systems and mount points can be displayed using `drives list mounted` and `drives list mountpoints` respectively.

A screen showing drives list mounted and drives list mountpoints:

```
platform@development:$ drives list mountpoints
Available mountpoints:
  core_services:SWAPSPACE
  core_services:appdata
platform@development:$ drives list mounted
Mounted drives:
  sdd1 - mongodb:dbroot
  sdc1 - core_services:backups
platform@development:$
```

The mount points are as follows:

- `mongodb:dbroot` is the volume used for database storage
- `core_services:backups` is used for default backup storage
- `core_services:appdata` is the main system volume used for application data in the users account
- `core_services:SWAPSPACE` is the swap volume used by the system
In order to add or extend an existing disk volume, follow the following steps:

- Under VMware, add an additional disk volume to the VM
- `drives list` displays any unused available volumes
- A free mountpoint can be linked to a new disk using `drives add <disk> <mountpoint>`.
- An existing used mountpoint (i.e., currently linked to a disk volume) can be linked to a new disk volume of greater size using `drives reassign <disk> <mountpoint>`. Existing data on the current disk will be copied to the new disk volume, and once successful, the new disk volume will be linked.

For example, the following steps can be followed to add a 250GB hard disk to the system:

1. Log into the VMware console and select Server.
2. Right-click and select Edit settings.
3. Click Add... and select Hard Disk.
4. Navigate through the rest of the wizard and edit parameters - in this case 250GB, thick provisioned.
5. Once done, log into the system as the platform user.
6. Execute a disk listing with the command `drives list`.
7. Reassign the disks with the command `drives reassign <new disk name> mongodb:dbroot`.
8. Start the application with `app start`.

SAN alignment is implemented using the offset value in `drives offset`. This value can be changed if necessary; however, the default should be sufficient for most SAN hardware.

For swap partitions, use `drives checkswap` to check their alignment. Use `drives alignswap` to fix a misaligned swap partition.
System Security

- Security, page 289
- Security Patches and Updates, page 290
- Using Your Own Repository Mirrors, page 290
- Configuration Encrypted, page 291
- Backup Encrypted, page 291
- Application Install Files Encrypted, page 291
- Protected Application Environments (Jails), page 292
- Restricted User Shell, page 292
- Creating Additional Users, page 292
- Granting and revoking user rights, page 293
- Password Strength Rules, page 294
- SSH key management, page 294

Security

The system defaults to a self-signed web certificate.

- A unique web certificate can be copied onto the host using `scp` or `system download`.
- The web certificate is installed using `web cert add <certificate file>`.

SSH keys are used for sftp, passwordless ssh and scp.

- Keys can be created using `keys createkey`.
- The public key copied to a remote host using `keys sendkey <user@host>`.
- A host can be authorized for incoming connections using `keys add <host>`.

The system uses an internal repository to check whether security package updates are available.
Additional repositories can be added with:

```
security repos add <repo-name> <url> <distro> <section> <categories>
```

For example, `security repos mymirror add http://archive.ubuntu.com/ubuntu/ precise-updates main universe multiverse`

In order to check whether there are security updates available, use:

```
security check
```

The system can be updated using:

```
security update
```

### Security Patches and Updates

During installation the system will automatically install the application named "security" which is a collection of all the latest security patches available for the various pieces of software in the platform at the time the system was built. Updates to this application are released to customers regularly. The security application provides these updates but does not automatically install them - allowing customers with concerns to verify them on lab machines first for example. Some security updates may also require scheduled downtime to complete and for this reason the final installation of updates is a manually triggered process.

The health command will inform the user if any security updates are currently available but not installed. Users can install security updates at any time by running the command:

```
security update
```

Those who would prefer to automate this can create a scheduled command to do so on a regular basis. The security update will install all operating system updates to both the main system and the application jails, but it will not generally contain updates to the core applications themselves - these are shipped separately as new application install versions as they require additional QA to ensure compatibility.

### Using Your Own Repository Mirrors

Some users may prefer to obtain security updates from the upstream distribution more frequently than they are repackaged by Cisco Unified Communications Domain Manager 10.6(1). This is fully supported by the security application.

From the command line, use the command:

```
security
```

to see the list of available command parameters.

Users can use the command:

```
security repos
```

to list current repositories from which updates are available.

Use the command:

```
security repos add <repo>
```

to add repositories from which updates are available. These repositories are in the same standard format as used by the underlying operating system.

For example on Ubuntu platforms they will resemble the following line:
security repos add http://security.ubuntu.com/ubuntu precise-security main restricted

You can point the system directly at the upstream provider or set up an internal mirror on your network which hosts only the updates you have approved, as long as the repository is network reachable by the platform it will function.

After adding your repositories you can check for any new available updates using the command:

security check

This command is also periodically run by the system itself and will report if any new updates are available. The command security update will install updates from your own repositories just as it would for the updates shipped with the platform.

To remove repositories, use the command:

security repos del <repo>

### Configuration Encrypted

In order to help protect customer data and service stability the system configuration files are frequently recreated by the platform. This means that even malicious tampering to the platform will generally be undone by a simple restart. The data used to do manage this is stored in the platform's internal configuration files. These files are encrypted using a strong AES encryption layer to make them tamper-proof. They are never decrypted on disk, instead the applications which manage them will decrypt them in memory, read and make modifications as needed and then re-encrypt the data before writing them back to disk.

In this way the risk of tampering or data theft through the configuration system is greatly minimized.

### Backup Encrypted

System backups include copies of the full system configuration as well as the full contents of the database. Thus theft of a backup would effectively constitute theft of all customer data stored on the platform. To mitigate this risk backups are encrypted using a strong 2048-bit in-line GPG encryption.

The encryption key for this is auto-generated by the platform based on a unique machine UUID. While it's possible for support to recover backups from a different machine this process is deliberately hard and only available to official technical support representatives. Backups on shared locations are separated on a per-source-machine basis to prevent conflicts.

### Application Install Files Encrypted

In order to protect the trustworthiness of applications shipped for the platform, all application installers are encrypted files. The strong 2048-bit key needed to decrypt these are shipped with the platform and is different from the per-machine unique keys used for other encryption tasks. This key will only decrypt applications encrypted specifically with the unique key owned by Cisco Unified Communications Domain Manager 10.6(1). The system will refuse to install any application that is not encrypted or encrypted with a different key.

This ensures that only valid, untampered copies of genuine Cisco Unified Communications Domain Manager 10.6(1)-released applications can be installed on the system.
Protected Application Environments (Jails)

Cisco Unified Communications Domain Manager 10.6(1) runs the service providing applications in secured jail environments. This has significant value for the security and reliability of the system. It prevents applications from cross-interfering which makes the system more stable and reliable. In terms of security it effectively confines all services to dedicated and separate mini file systems with predictable content. In the event that an attacker were to gain access to the system through a vulnerability in a service he would therefore not gain access to the platform but only to the small confined jail in which the service was running. In that environment only the jail itself is vulnerable and this can be very easily restored if damaged. The underlying system cannot be accessed from the jailed environment.

Restricted User Shell

The platform attempts to reduce the risk of unintentional harm to the operation of the software by restricting the actions users can take. This is done using a specially configured setup of the well-known and actively maintained bash shell.

The shell actively prevents the following:

- Users cannot set environment variables or alter their command path.
- Users cannot change the current directory.
- Users cannot specify a path to a command to run.

The commands users thus are able to run is only what is allowed by the platform setup. The vast majority of these commands use a common execution interface designed to allow only enough privileges to perform the system administration tasks they are created for. The exact list of commands a user can run is determined by his specific privileges and the specific setup of the machine on which he is working (different applications can add their own additional commands). This list is displayed on login and can be redisplayed with the help command.

Creating Additional Users

During installation a user called 'platform' is created which has full access to all allowed commands within the restricted environment. This user (and others with the appropriate rights) can then create additional users who are further restricted to only be able to run certain commands. For example a user could be created who can only run diagnostic and logging commands - able to monitor the health of a system but required to escalate any actions.

Users are created, managed and deleted through the user command. To create a new user use:

```bash
user add <username>
```

The system will create a Unix user with the name specified and set up to use a restricted shell identical to the platform user. Initially this user's password is set to match the username but it must be changed on first login. New users start out with no rights and can only run the very basic system commands provided to all users (such as `ls`).
Granting and revoking user rights

Once a user is added the user needs to be granted access to run commands. The user's command menu will only display those commands to which access have been granted.

To grant access to a command use the 'user grant' command as follows:

```
user grant <username> <command> [options]
```

Only one command can be granted at a time, however these can be complex. The more detailed the command, the more fine-grained the privilege becomes. This is best explained by example.

Running the following command:

```
user grant peter app
```

Will allow the user peter to execute any command within the 'app' series of commands. However it could be restricted further by instead running a command like:

```
user grant peter app list
```

With this version peter will see the app command on his menu, but its help will only display 'list' as a sub-command - peter can thus see the list of apps but cannot perform more potentially risky tasks such as installing or restarting applications.

This can be expanded to other subsets by simply running additional grants:

```
user grant peter app start
```

Would now allow peter to both see the list of applications or restart applications that failed, however he will not be able to do other app related tasks such as installations. The grant command effectively verifies that the start of a command by a user matches one of the privileges granted to that user - so peter will be able to add options to any command he is granted access to.

In order to restrict commands - be sure to determine whether any options should be allowed and if not, only grant access to the specific parameters you wish peter to be able to execute. For example if peter is your database administrator for example you may wish to use:

```
user grant peter app start mongodb
```

Instead of giving access to all app start commands.

Should you wish to revoke a command privilege from a user you can do this using the following command:

```
user revoke <username> <full command>
```

The command being revoked must match exactly one of the commands previously granted to a user. To review the current privileges of a user use:

```
user list <username>
```

Which will display the user's entire list of granted commands in full. You can also just run

```
user list
```

Without an option to list all users created on your system and their privileges.
Password Strength Rules

The platform user and any users created are held to strong password rules to help reduce the risk of system penetration. These rules are enforced whenever passwords are changed or set. In order to meet system password strength rules a user's password must:

- Be at least 16 characters long.
- Contain at least one capital and one non-capital letter.
- Contain at least one number.
- Contain at least one special character.

SSH key management

SSH authentication requires maintaining the system SSH keys. This can be done as follows:

- `keys create` creates a local SSH keyset
- `keys send <user>@<host>` will send the public key from the local SSH keyset to the remote server, thereby enable remote SSH authentication.
- `keys add <host>` adds the remote host to the known hosts list allowing outgoing connections

For example, if you wish to perform a backup to a remote host, first create a local key if necessary with `keys create`. Allow communication with the host using `keys add <host>`. Send the key to the remote host with `keys send <user>@<host>`.

The certificates are independent of web servers/proxies.

For more details on SSH key-based authentication, refer to OpenSSH documentation.
Network Security

- Network Communications between Nodes within the Cluster, page 295
- Network Communications External to the Cluster, page 297
- Dynamic Firewall, page 298
- Service and Ports list, page 298
- Web Certificates, page 299
- Web Certificate Expiration Notice, page 299
- Set Up a Web Certificate, page 300
- Web Certificate Commands, page 300
- Network URI specification, page 300

Network Communications between Nodes within the Cluster

The following details are all based on the default settings. These can vary depending on the application setup and network design (such as NAT) of the solution, so may need adjustment accordingly. Where a dependant is noted, this is fully dependant on the configuration with no default.

These communications are all related to communications between application nodes within the cluster. There are a few different deployment models so the details below cover the different models and relevant ports. So review and implement according to the deployment model in use.

Note

Standalone is only a single node so this section is not relevant for that deployment model.

Proxy to Proxy Node

This is relevant if the proxy node is present in the system.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Communications</td>
<td>HTTPS</td>
<td>TCP 8443 bi-directional</td>
</tr>
</tbody>
</table>
## Network Communications between Nodes within the Cluster

### Proxy to Unified/Application Node
This is relevant if the proxy node is present in the system.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>User access</td>
<td>HTTPS</td>
<td>TCP 443</td>
</tr>
<tr>
<td>Cluster Communications</td>
<td>HTTPS</td>
<td>TCP 8443 bi-directional</td>
</tr>
</tbody>
</table>

### Unified Node to Unified node
This is relevant to the communications between the unified nodes (application and database combined). If the application and database nodes are split, then see the relevant application and database node details below. Database arbiters run on port 27030.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database access</td>
<td>database</td>
<td>TCP 27017 and 27030 bi-directional</td>
</tr>
<tr>
<td>Cluster Communications</td>
<td>HTTPS</td>
<td>TCP 8443</td>
</tr>
</tbody>
</table>

### Application node to Application node
This is relevant to the communications between application nodes in the system. This is only relevant where the database node is separate from the application node (in other words, not Unified node).

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster communications</td>
<td>HTTPS</td>
<td>TCP 8443 bi-directional</td>
</tr>
</tbody>
</table>

### Application Node to Database node
This is relevant to the communications between the application node and the database node. This is relevant if the database node is separate from the application node. Database arbiters run on port 27030.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database access</td>
<td>database</td>
<td>TCP 27017 and 27030 bi-directional</td>
</tr>
<tr>
<td>Cluster Communications</td>
<td>HTTPS</td>
<td>TCP 8443</td>
</tr>
</tbody>
</table>

### Database Node to Database node
This is relevant to the communications between the application node and the database node. This is relevant if the database node is separate from the application node. Database arbiters run on port 27030.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database access</td>
<td>database</td>
<td>TCP 27017 and 27030 bi-directional</td>
</tr>
</tbody>
</table>
Network Communications External to the Cluster

The following details are all based on the default settings. These can vary depending on the application setup and network design (such as NAT) of the solution, so may need adjustment accordingly. Where a dependant is noted, this is fully dependant on the configuration with no default.

These communications are all related to communications with devices external to the cluster.

Outbound Communications to Devices from the Application/Unified nodes:

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager (UCM)</td>
<td>HTTPS</td>
<td>TCP 8443</td>
</tr>
<tr>
<td>Cisco Unity Connection (CUXN)</td>
<td>HTTPS</td>
<td>TCP 8443</td>
</tr>
<tr>
<td>Webex</td>
<td>HTTPS</td>
<td>TCP 443</td>
</tr>
<tr>
<td>LDAP directory</td>
<td>LDAP</td>
<td>TCP/UDP 389 and/or 636(TLS/SSL)</td>
</tr>
<tr>
<td>Single Sign-on (SSO)</td>
<td>HTTPS</td>
<td>TCP 443</td>
</tr>
<tr>
<td>Cisco HCM-F</td>
<td>HTTPS</td>
<td>TCP 8443</td>
</tr>
</tbody>
</table>

Outbound to external systems from the proxy node:

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Network Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Sync and Async responses</td>
<td>HTTPS</td>
<td>TCP 443</td>
</tr>
<tr>
<td>Northbound Notification messages</td>
<td>HTTPS</td>
<td>dependant</td>
</tr>
</tbody>
</table>

Outbound to external systems from all nodes:

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>SNMP</td>
<td>TCP/UDP 162</td>
</tr>
<tr>
<td>SFTP as required for backup destinations</td>
<td>SFTP</td>
<td>TCP 22</td>
</tr>
<tr>
<td>NTP</td>
<td>NTP</td>
<td>UDP 123</td>
</tr>
</tbody>
</table>
Inbound communications from external systems to the proxy node:

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Access</td>
<td>HTTPS</td>
<td>TCP 443</td>
</tr>
<tr>
<td>API Request</td>
<td>HTTPS</td>
<td>TCP 443</td>
</tr>
</tbody>
</table>

Inbound communications to all nodes:

<table>
<thead>
<tr>
<th>Communication</th>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH and SFTP for management and files transfers</td>
<td>SFTP/SSH</td>
<td>TCP/UDP 22</td>
</tr>
</tbody>
</table>

Dynamic Firewall

The most important part of the network security model is the system firewall.

The platform uses a dynamic firewall which does not open a fixed set of ports but adapts to the applications installed, only allowing such traffic as the specific set of running services require.

If an application is stopped, its ports are automatically closed. This creates a default-blacklist firewall which pinholes only those ports required for the operation of the specific setup in use.

The firewall is one of the very first services the platform brings up and among the very last it shuts down in order maximize the network security.

Where possible, the firewall will also rate limit connections to services to prevent abuse (see the section: Prevention of DOS attacks for more details).

Service and Ports list

The following external network ports are in use and need to be opened on the firewall for communication between cluster nodes:

<table>
<thead>
<tr>
<th>Node type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebProxy</td>
<td>22 (ssh &amp; sftp), 80 (http), 161 &amp; 162 (snmp), 443 &amp; 8443 (https)</td>
</tr>
<tr>
<td>Application</td>
<td>22 (ssh &amp; sftp), 80 (http), 161 &amp; 162 (snmp), 443 &amp; 8443 (https), 27017 &amp; 27030 (database)</td>
</tr>
<tr>
<td>Database</td>
<td>22 (ssh &amp; sftp), 161 &amp; 162(snmp), 27019 &amp; 27020 (database)</td>
</tr>
</tbody>
</table>

Additionally, the Application node interacts with external Cisco equipment (e.g. UCM, CUCx) and will require additional firewall ports to be opened.
Web Certificates

The platform installs a self-signed certificate for the web-frontend by default. This provides encryption of the web-traffic but does not provide users with valid authentication that the server is correct or protect against man-in-the-middle attacks.

For this reason we strongly advise customers to obtain a trusted CA-signed certificate and install it on the server. Once a signed, trusted certificate is obtained (this should be a single-file concatenated certificate suitable for the NginX server) copy it to the platform using scp and then install the file into the server using:

```
web cert add <filename>
```

Only one certificate file can be installed on the platform. For more details on NginX compatible certificates see the relevant nginx documentation here: [http://wiki.nginx.org/HttpSslModule](http://wiki.nginx.org/HttpSslModule)

Please note the importance of ensuring that SSL certificates generated match the assigned network name of the platform.

Web Certificate Expiration Notice

If a Web Certificate is due to expire, a notice will display on the status display 30 days before the expiration:

```
WEB CERT EXPIRES AT: 2014-09-26 11:30:02
```

If a Web Certificate has expired, the notice on the status displays:

```
WEB CERT EXPIRED AT: 2014-09-26 11:30:02
```

Once the certificate is expired, the system can be used as normal, but the certificate will be expired and for non self-signed certificates (like a Godaddy or Thawte certificates), the data will no longer be properly encrypted.
Set Up a Web Certificate

Procedure

Step 1 Run `web cert details` if needed to edit the details displayed from the server.
Step 2 Run `web cert gen_csr` to generate the Certification Request (CSR).
Step 3 Send the file to a Certificate Authority (CA).
Step 4 Upload the reply from the CA to the server using `scp`.
Step 5 Run `web cert add <filename of uploaded file>`.

Web Certificate Commands

The following Command Line Interface console display shows the available commands for web certificates.

- `web cert add <filename>` - Install the certificate from `<filename>` into the web server.
- `web cert del` - Revert to a self-signed certificate
- `web cert details` - Print the certificate details in config system.
- `web cert details edit` - Update the certificate details in config system.
- `web cert gen_csr` - Create a CSR file in /opt/platform/admin/home/media.
- `web cert gen_selfsigned` - Generate a self-signed certificate.
- `web cert print_csr` - Create a CSR file in /opt/platform/admin/home/media.
- `web cluster prepnode` - Prepares the system so that it can be joined to a cluster as a web proxy.
- `web sslv3 <on/off>` - Enable/disable SSLv3 on the system.
- `web weight add <server:port> <weight>` - Modify the weights of an upstream service. Higher weights will serve more requests, while 0 will only be used if no other servers are available.
- `web weight del <server:port>` - Delete the user-defined service weight and use system defaults.
- `web weight list` - Display the weights of upstream services

Network URI specification

All network locations are specified as a URI, for example download locations, backup destinations, notification destinations, and so on.

The following list shows the URI syntax:

- `ftp: ftp://user[:password]@host[:port][/path]`
- `http: http(s)://user[:password]@host[:port]/path`
• **file**: `file://[/path]+[/filename]

• **sftp**: `sftp://user[:password]@host[:port][/path]

• **scp**: `scp://[user@]host[:port]:[/path]

• **Email**: `mailto:user@host

• **snmpv2**: `snmp://community@host[:port]

• **snmpv3**: `snmp://user:auth:password]@host[:port] ... minimum auth/password
Macros

- Macros, page 304
- Macro Syntax Brackets, page 304
- Dot notation, page 305
- SELECT FROM WHERE Macro Syntax, page 306
- Macro Nesting, page 310
- Macro Syntax to Filter by Meta Properties, page 310
- Numeric Functions, page 312
- String Functions, page 312
- List Functions, page 314
- Rule Filter Functions, page 317
- Macro Function, page 319
- CUCM Functions, page 319
- Subscriber Functions, page 320
- Zero, Unset and Boolean Functions, page 321
- Time Functions, page 321
- Hierarchy Functions, page 323
- Request Functions, page 324
- Internal Number Inventory Functions, page 324
- Localization Functions, page 327
- Log Functions, page 328
- Object Keys Functions, page 329
- Macro and Macro Function Nesting, page 330
- Conversion Functions, page 330
- Conditional Logic Macro Function, page 331
Macros

Macros are used to return data from the system in various formats, to test for conditions, map data from GUI or bulk loader input to various elements in the system (in conjunction with configuration templates) and to access data in workflow and wizard steps.

Various macro functions are available. These serve as boolean operators or can be used to carry out various numeric functions, string manipulation functions, list functions, time functions, and hierarchy related functions.

Macros can be created for re-use, named and stored as an instance of the Macro data model. When re-used, the reference prefix syntax is of the format: macro.<macroname>.

Named macros and macro functions can be nested within other macros.

Macro Syntax Brackets

Macros can have any of the following markup:

- {{ and }} indicate macros that resolve to single values.
  The value can also return an object. A direction parameter is also available for hierarchy searching. This is indicated by ||.
- {# and #} indicate macros that resolve to lists of values.
- %{% and %} indicate macros that resolve to dictionaries.
- (( and )) indicate macros that test for a condition are enclosed in round brackets ((and )) - these macros evaluate to True or False.
  The comparison operators that are available for these macros are: ==, !=, <, >, <=, >=.
  The OR operator in a test is |, for example:
  
  
  ```
  ( ( device.cuc.PagerDevice.Undeletable|ObjectId:input.ObjectId|
    direction:local == False ) )
  ```
- ((test)) <if value> <else value> - IF ELSE type conditional macro.
- ((test)) <value> ((test)) <value> <value> - IF ELSEIF ELSEIF-type macros combine tests and result values if the test resolves to True or False. The logic is IF (test) THEN <value> ELSE IF (test) THEN <value> ELSE <value>.
Example:

```{(self.a == self.b)} <foo>{{CallManager.host}}</foo>```

```{(self.b == self.c)} <foo>{{CallManager.username}}</foo>```

```<foo>{{CallManager.version}}</foo>```

This macro tests for the equality of values in a calling model (referenced by 'self') and returns an evaluation for the condition that is True. The evaluation refers in dot notation to attributes of a Data Model called 'CallManager' and concatenates the result with a string 'foo-'.

- ‘SELECT FROM WHERE'-type macros returning single-, dictionary- and list type values and can take parameters. The format is:
  ```* {SELECT FROM | WHERE *
  * %{SELECT FROM | WHERE %}
  * #{SELECT FROM | WHERE #}```

### Dot notation

A dot-notation is used to refer to a macro function, model attribute, a defined variable, step reference, or non-attribute value in the model schema.

- **fn.macrofunction**._name_ - identifies a macro function.
- **self.attribute** - used to refer to the current value of an attribute in the model where the macro applies.
  Here, _attribute_ should be an attribute name of the calling model in which the macro is referenced (usually a configuration template). In other words, the macro should be associated with a configuration template of a resource that is referenced.
- **previous.attribute** - used to show the previously saved value of an attribute as opposed to the existing value in the case where a model is updated.
- **input.attribute** - the values input via any of the GUI, or bulk load, for each variable or context..
- **pwf.variablename** - identifies a variable value defined as a provisioning workflow set step variable.
- **cft.attribute** - identifies the values input in a Configuration Template via the current value of the _context_var_ of a foreach loop in the Configuration Template.
- **modelname.attribute** - this notation defaults to the Data Model type.
- **modeltype.modelname.attribute** - is used for other non-data model types.
- **modeltype.modelname.attribute.NUMBER** - is used to refer to attribute NUMBER-1 where there is more than one attribute, that is, the first attribute reference is **modeltype.model.name.attribute.0**.
- **macro.name** - used to refer to a defined macro by name.
- **workflow.stepSTEPNUMBER.pkid** - used to override the Context Hierarchy by specifying the context using the pkid of stepSTEPNUMBER, where STEPNUMBER can be 1,2 and so on.

Non-attribute notation allows the following for a model:
  ```* __pkid```
Some examples of this syntax:

- `{# data.Countries__pkid #}`
- `{# data.CallManager.__bkey #}
- `{data.CallManager.__bkey | host: 172.29.248.150 }
- `{data.CallManager.__hierarchy | host:172.29.248.150 }
- `{data.CallManager.__hierarchy_friendly_path | host:172.29.248.150 }
- `{data.CallManager.__hierarchy_friendly_parent_path | host:172.29.248.150 }

Meta attribute properties can also be used in a macro filter.

- To indicate sequence instance with SEQ - the value is a loop sequence number starting from 1 or a wizard step number:
  - It is obtained from a **Foreach List Macro** in a Provisioning Workflow or a **Foreach Elements** loop in a Configuration Template.
    
    This value can be used to refer to an attribute of a model. An array item in a Configuration Template has a **Foreach Elements** loop with a variable *phoneX*:
    
    `{# self.Phone.{{fn.subtract input.phoneX.SEQ, 1}}.lines.line #}`

    that refers to an attribute (line in a list of phones), starting with the first one:

    `self.Phone.0.lines.line`

    - This value can be used to refer to a Wizard step (stepSTEPNUMBER) in its Configuration Template. A **Foreach Elements** loop with a variable *step* that holds a list of STEPNUMBER obtained from the wizard:

    `{# input.define_wizard_steps #}`

    so that stepSTEPNUMBER can be incremented with:

    `step{ {cft.step.SEQ} }`

### SELECT FROM WHERE Macro Syntax

The types of return values are indicated by the syntax:

- `{ {SELECT FROM | WHERE}}` for single values or objects
- `{{%SELECT FROM | WHERE%}}` for dictionaries
- `{#{SELECT FROM | WHERE#}` for lists

The SELECT FROM part is a model reference and uses dot notation.
For lists and dictionaries, the SELECT FROM notation can contain a wildcard asterisk * to return all matching values.

Examples returning all User attributes:

```{# User.* | username: js54321, last_name: 'van Dever' #}
{# User.* | username: js54321 %}
```

The WHERE part is one or more comma-separated name:value pairs of attribute values of the model reference. If the value itself has a comma, it should be wrapped in quotes.

For example:

```{{ data.Countries.* | country_name: 'India, Republic of' }}
```

The value can also contain:

- A reference to a defined macro used to return a value, as in:
  ```{# data.DRTPBXMeta.* | PBX:macro.getHost #}
  ```
- A boolean value using the corresponding macro function, as in:
  ```{{ data.DATA1.name | code: fn.true }}
  ```

The WHERE part also supports:

- Asterisk "*" for filtering.

Examples:

```{{ device.cucm.Phone.lines.line | name: "SEPD13B004F0719", lines.line.*.dirn.pattern: "1006", lines.line.*.dirn.routePartitionName: "AllowEmerCalls-NewSite4" }}
```

If there is a "*" in the WHERE clause:

- the results list is reduced with that specific clause
- the specific WHERE clause is a list

Note that only one "*" supported and if the WHERE clause has an invalid field name, it will be ignored and still return the data.

- regular expression type syntax:

  ```field:/regex/
  ```

  Example:

  ```{# data.Countries.country_name | country_name:/ia$/ #}
  ```

  returns names that end in "ia":

  ```[ "Australia", "Saudi Arabia" ]
  ```

  Similarly, to exclude a list of countries matching "ia" in the name:

  ```{# data.Countries.country_name | country_name:/[^ia]$/ #}
  ```
Macros cannot be nested in the regex. This will **not** work:

```# data.Countries.* | iso_country_code: /[^{{input.ISO}}]/ #```

But this will work:

Macro ISO_REGEX:

`/[^{{input.ISO}}]/`

Macro:

```# data.Countries.* |
iso_country_code:macro.ISO_REGEX #```

- attributes not in the data of the model schema
  - `__pkid`
  - `__bkey`
  - `__hierarchy`
  - `__hierarchy_friendly_path`
  - `__hierarchy_friendly_parent_path`

For example, given the following:

Macro USA_pkid:

```{{ data.Countries.__pkid | iso_country_code:USA }}
```

Then Macro:

```{{ data.Countries.country_name | __pkid:macro.USA_pkid }}
```

will return

"United States of America"

Note that when using `__hierarchy_friendly_path` in a WHERE clause, the option clause direction will be ignored, for example:

```# data.Countries. | __hierarchy_friendly_path: sys.TestMacros #```

will only return Countries at this hierarchy node.

The SELECT-FROM-WHERE macros can also take additional parameters that restrict results:

- `direction:[up|down|local|parent|below|above]`
- `device:[pkid of device]`
- `ndl:[pkid of ndl]`

The direction option can be added to return values relative to the current hierarchy position. The default direction is down:

- `direction:up` - Upwards. Include current hierarchy.
- `direction:down` - Downwards. Include current hierarchy.
- `direction:local:` - On this level only. Include current hierarchy.
• **direction:parent** - Parent only. Exclude current hierarchy, in other words, search the parent as local.

• **direction:below** - Downwards. Exclude current hierarchy.

• **direction:above** - Upwards. Exclude current hierarchy.

In a 'SELECT-FROM-WHERE'-type macro, a single bar indicates the direction, for example:

```{% data.Countries|iso_country_name:AUS|direction:up %}
```

If used in other macro types, a double bar is used for parameters, for example:

```#{ data.SiteDefaultsDoc.defaultcucphonesystem || direction:local #}
```

When traversal is *up* or *above*, results will be ordered starting with ones at the lowest hierarchies. Otherwise, results will be ordered starting with the ones at the highest hierarchies. Results at the same hierarchy will be in arbitrary order.

Added to the direction option is an optional limit specifier. When used, the results returned by a list comprehension will be limited to the specified count, for example:

```#{ data.test_user.name || direction:above,limit:2 #}
```

This will return the first two names of *data/test_user* instances at the closest ancestors.

By default, for the following filter specifiers values apply to lists if they are not present:

- **skip** (default: 0) - skip over a number of values before listing

- **limit** (default: 2000) - number of values to return in the list

So, if the first list macro was:

```#{ data.test_user.name || skip:0,limit:2000 #}
```

then the second batch of results can be obtained by:

```#{ data.test_user.name || skip:2000,limit:2000 #}
```

In addition, a **title** filter can be applied if the SELECT-FROM query is for a string to only return values matching its value, with a regular expression, for example:

```#{ data.Countries.country_name||title:.*of$ #}
```

returns:

```[
"India, Republic of","Oman, Sultanate of","Qatar, State of","Singapore, Republic of","Sweden, Kingdom of"]
```

Device option:

A device or ndl (Network Device List) pkid can be specified to restrict a query, for example, assume a named macro **MY_CUCM_PKID_150**: 

```{{ data.CallManager.__pkid | host:172.29.248.150,port:8443 }}
```

then we can select from the specified device as follows:

```{{ device.cucm.HuntList.__pkid | name: "DR-Test1" | device:macro.MY_CUCM_PKID_150 }}
```

```{{ device.cucm.HuntList.__hierarchy | name: "DR-Test1" | device:macro.MY_CUCM_PKID_150 }}
```
In a GUI Rule, [ and ] indicate references to values in the current usage context of the GUI Rule if the macro is added as a Value to the GUI Rule.

A GUI rule Action can also have an API call as its Source. The references are current context hierarchy pkid’s or to field attribute names in the WHERE section of SELECT FROM WHERE-type macros - enclosed in square brackets [ ].

For example:
/api/tool/Macro/?method=evaluate&hierarchy=[hierarchy]
&input={{Countries.iso_country_code | country_name:[countries.name]}}

The syntax in a GUI Rule for a Wizard also uses [], in the format [stepData.STEPNAME.ATTRIBUTE], for example:
[stepData.SubscriberType.role]

Macro Nesting

To nest macro calls, create a named macro. Nesting inside macros is not supported.

For example, the following incorrect macro:

```
(( fn.list_in Kit, {# fn.split {{ fn.one device.ldap.user.streetAddress | sAMAccountName: bjones }} #} == True)).
```

should be split up into named macros:

- **macro: LDAP_USER**

```
{{fn.one device.ldap.user.streetAddress | sAMAccountName: bjones }}
```

- **macro: LDAP_USER_ADDRESS_LIST**

```
{# fn.split macro.LDAP_USER #}
```

So the correct macro usage should be:
```
(( fn.list_in Kit, macro.LDAP_USER_ADDRESS_LIST == True))
```

Macro Syntax to Filter by Meta Properties

Macro results can also be filtered by the meta data of a resource.

A typical resource instance has associated meta data, for example:

```
meta: {
title: "Australia - AUS"
cached: true
tags: [0]
schema_version: "0.1.5"
summary: "true"
references: {...}
```
The following macro fields are supported to filter by these properties:

- `__meta.business_key`
- `__meta.model_type`
- `__meta.schema_version`
- `__meta.system_resource`
- `__meta.tags`
- `__meta.title_format`
- `__meta.uri`
- `__meta.version_tag`

The macro fields can be combined with model attribute names in a comma separated, for example:

```
#{ data.Countries.country_name, __meta.schema_version | country_name:Australia #}
```

Output:

```
[
 {
  "country_name": "Australia",
  "__meta": {
    "schema_version": "0.1.5"
  }
 }
]
```

As a further example: if the `system_resource` is set in the `meta` section of the resource, then the following macro can be used:

```
#{ data.ConfigurationTemplate.name | __meta.system_resource: true #}
```

The output is all the Configuration Template names where it is a system resource:

```
 ]
```

For devices, the following are examples of macros that are available for the device NDL:

```
__device_meta.ndl.name
__device_meta.ndl.data/CallManager.pkid
```
Numeric Functions

- **fn.zeropad** - Left pad a given number with zeros up to a given pad number.
- **fn.minval** - For integers, return the minimum value of a provided list.
- **fn.maxval** - For integers, return the maximum value of a provided list.
- **fn.add** - Add two integers.
- **fn.subtract** - Subtract two integers.
- **fn.multiply** - Multiply two integers.
- **fn.divide** - Divide two integers.

Examples:

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>{{fn.zeropad 123,6}}</td>
<td>000123</td>
</tr>
<tr>
<td>{{fn.minval 2,3,130,1,30}}</td>
<td>1</td>
</tr>
<tr>
<td>{{fn.maxval 2,3,130,1,30}}</td>
<td>130</td>
</tr>
<tr>
<td>{{fn.add 2,3}}</td>
<td>5</td>
</tr>
<tr>
<td>{{fn.subtract 2,3}}</td>
<td>-1</td>
</tr>
<tr>
<td>{{fn.multiply 2,3}}</td>
<td>6</td>
</tr>
<tr>
<td>{{fn.divide 20,10}}</td>
<td>2</td>
</tr>
</tbody>
</table>

String Functions

- **fn.index** - Return the i’th item of an iterable, such as a list or string.
- **fn.mask** - Return a mask of (length + modifier) instances of char.
- **fn.length** - Return the length of a string.
- **fn.split** - Split a string by delimiter, returning a list.
- **fn.join** - Join a string by delimiter. If no delimiter is provided, the list is returned as a single string.
- **fn.title** - Return a string in title case.
- **fn.upper** - Return an uppercase version of the input string.
- **fn.lower** - Return a lowercase version of the input string.
- **fn.contains** - Return true or false if string is contained in another.
- `fn.sub_string` - Return the substring of a string from a start to an end position.
- `fn.containsIgnoreCase` - Return true or false if string is contained in upper- or lower case.
- `fn.containsStartsWith` - Return true or false if source string is the start of target string.
- `fn.containsStartOf` - Return true or false if start of source string is target string.
- `fn.isexactly` - Return true or false if source string is exactly the same as target string.
- `fn.replace` - Replace target substring for source substring in source string.

Examples:

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{fn.index 'foo bar baz', 5}</code></td>
<td>'b'</td>
</tr>
<tr>
<td><code>{fn.mask X, 2, 3}</code></td>
<td>XXXXX</td>
</tr>
<tr>
<td><code>{fn.length This is a valid string}</code></td>
<td>22</td>
</tr>
<tr>
<td><code>{# fn.split foo/bar/baz,/#}</code></td>
<td>['foo', 'bar', 'baz']</td>
</tr>
<tr>
<td><code>{ fn.join 1234; }</code></td>
<td>1:2:3:4</td>
</tr>
<tr>
<td><code>{ fn.join 1234 }</code></td>
<td>1234</td>
</tr>
<tr>
<td><code>{fn.title 'foo bar baz'}</code></td>
<td>'Foo Bar Baz'</td>
</tr>
<tr>
<td><code>{fn.upper somevalue}</code></td>
<td>SOMEVALUE</td>
</tr>
<tr>
<td><code>{fn.lower SOMEVALUE}</code></td>
<td>somevalue</td>
</tr>
<tr>
<td><code>{fn.contains needle, haystack}</code></td>
<td>false</td>
</tr>
<tr>
<td><code>{fn.contains hay, haystack}</code></td>
<td>true</td>
</tr>
<tr>
<td>(( fn.contains Kit, 1234 Kit Creek == True ))</td>
<td>true</td>
</tr>
<tr>
<td><code>{fn.sub_string haystack 0, 2}</code></td>
<td>hay</td>
</tr>
<tr>
<td><code>{fn.sub_string haystack 7, 7}</code></td>
<td>k</td>
</tr>
<tr>
<td><code>{fn.containsIgnoreCaseaaa, bbbaAaccc }</code></td>
<td>true</td>
</tr>
<tr>
<td><code>{ fn.containsStartsWith aaa, aaaaAaccc }</code></td>
<td>true</td>
</tr>
<tr>
<td><code>{ fn.containsStartOf ffnncgg, ffnn }</code></td>
<td>true</td>
</tr>
<tr>
<td><code>{ fn.isexactly source1, source1 }</code></td>
<td>true</td>
</tr>
<tr>
<td><code>{ fn.replace ddddaAAAc,AAA,FFF }</code></td>
<td>ddddfFFFf</td>
</tr>
</tbody>
</table>
List Functions

- fn.list_index: Return a specified item from a list. Zero is the first item.
- fn.list_index_item: Return the position of item in list.
- fn.list_count: Return the number of items in a list. Note that if the list is known and empty, the count is 0, but if the list is not known, then the count is 1, because the returned message string count is 1.
- fn.list_count_item: Return the number of times item is in a list.
- fn.list_contain: Return true or false if item is in a list or not.
- fn.list_append: Returns a list with item appended.
- fn.list_pop: Return the last item of the list.
- fn.list_insert: Return a list with item inserted at position.
- fn.list_insert_no_dup: Return a list with item inserted at position and all duplicates ignored.
- fn.list_remove: Return a list with all instances of item or list of items removed.
- fn.list_remove_dup: Return a list with all instances of item or list of items removed, including duplicates.
- fn.list_reverse: Return a list that is the reverse of a given list.
- fn.list_extend: Return a list that is an extension of list 1 with list 2.
- fn.list_extend_no_dup: Return the concatenation of list1 and list2, ignoring duplicates.
- fn.sequence: Return a sequence of numbers running from the first value to the second value, optionally padded with zeroes to be the length of a third value.
- fn.list_sort: Return a sorted list; by ascending (A) or descending (D) order.
- fn.one: Return a single result from a list. This is used to convert a single element list to a string. If fn.one is called with a string, it returns the string unchanged. The string can be a macro that might get the value of another attribute from a context, such as input.some_variable.
- fn.as_list: Return a string result as a list. If fn.as_list is called with a string, it returns a list. Again, abc could be a macro that resolves to the value of an attribute in its context.
- fn.list_empty: Returns an empty list.
- fn.list_set_intersect: Given two lists, return the intersection as a list.
- fn.list_set_union: Given two lists, return the union as a list.
- fn.list_set_left: Given two lists, return a list of items in the left list only.
- fn.list_set_right: Given two lists, return a list of items in the right list only.

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{{fn.list_index 2, data.Countries country_name}}</code></td>
<td>“Canada” if this is the third item.</td>
</tr>
</tbody>
</table>
### Example

<table>
<thead>
<tr>
<th>MACRO1={# fn.sequence 40, 43 #}</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>{{ fn.list_index_item 42, macro.MACRO1 }}</td>
<td>2</td>
</tr>
<tr>
<td>{{ fn.list_index_item 42, macro.MACRO1 }}</td>
<td>25 if the list has 25 items.</td>
</tr>
<tr>
<td>{{ fn.list_count data.Countries }}</td>
<td>0</td>
</tr>
<tr>
<td>{{ fn.list_count input.does_not_exist }}</td>
<td>1</td>
</tr>
<tr>
<td>{{ fn.list_count non_existant_namespace.does_not_exist }}</td>
<td></td>
</tr>
<tr>
<td>MACRO1={# data.Countries. international_access_prefix #} {{ fn.list_index_item 00, macro.MACRO1 }}</td>
<td>19</td>
</tr>
<tr>
<td>{{ fn.list_contain 'AUS', data.Countries.iso_country_code }}</td>
<td>true</td>
</tr>
<tr>
<td>{{ fn.list_contain 'AUZ', data.Countries.iso_country_code }}</td>
<td>false</td>
</tr>
<tr>
<td>MACRO1={# fn.sequence 40, 43 #} {{ fn.list_append 999, macro.MACRO1 }}</td>
<td></td>
</tr>
<tr>
<td>MACRO1={# fn.sequence 40, 43 #} {{ fn.list_pop macro.MACRO1 }}</td>
<td>43</td>
</tr>
<tr>
<td>MACRO1={# fn.sequence 40, 43 #} {{ fn.list_insert 1, 999, macro.MACRO1 }}</td>
<td></td>
</tr>
<tr>
<td>MACRO1={# fn.sequence 40, 43 #} MACRO7={# fn.sequence 39, 41 #} {{ fn.list_insert_no_dup macro.MACRO1, macro.MACRO7 }}</td>
<td></td>
</tr>
<tr>
<td>MAC1={# fn.sequence 40, 43 #} MAC7={# fn.sequence 40,41 #} MAC3={{ fn.list_insert 1,43, macro.MAC1 }} {{ fn.list_remove 43, macro.MAC3 }} {{ fn.list_remove macro.MAC7, macro.MAC1 }}</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>Output</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Given the following list is the result of the regex for</td>
<td>['AUS', 'SAU']</td>
</tr>
<tr>
<td>iso_country_code:</td>
<td></td>
</tr>
<tr>
<td>{{# data.Countries.</td>
<td></td>
</tr>
<tr>
<td>iso_country_code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iso_country_code:/AU/ #)</td>
</tr>
<tr>
<td></td>
<td>['AUS', 'SAU', 'AUS', 'AUS']</td>
</tr>
<tr>
<td>{{# fn.list_remove_dup</td>
<td></td>
</tr>
<tr>
<td>data.Countries.</td>
<td></td>
</tr>
<tr>
<td>iso_country_code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iso_country_code:/AU/ #)</td>
</tr>
<tr>
<td>MACRO1={{# fn.sequence 40, 43 #}</td>
<td>['43', '42', '41', '40']</td>
</tr>
<tr>
<td>{{fn.list_reverse macro.MACRO1}}</td>
<td></td>
</tr>
<tr>
<td>MACRO1={{# fn.sequence 40, 43 #}</td>
<td>['40', '41', '42', '43', '50', '51', '52']</td>
</tr>
<tr>
<td>MACRO9={{# fn.sequence 50, 52 #}</td>
<td></td>
</tr>
<tr>
<td>{{fn.list_extend macro.MACRO1, macro.MACRO9}}</td>
<td></td>
</tr>
<tr>
<td>MACRO1={{# fn.sequence 40, 43 #}</td>
<td>['40', '41', '42', '43', '44', '45']</td>
</tr>
<tr>
<td>MACRO8={{# fn.sequence 42, 45 #}</td>
<td></td>
</tr>
<tr>
<td>{{fn.list_extend_no_dups  macro.MACRO1, macro.MACRO8}}</td>
<td></td>
</tr>
<tr>
<td>{{# fn.sequence 40, 43 #}</td>
<td>['40', '41', '42', '43']</td>
</tr>
<tr>
<td>{{# fn.sequence 110, 100, 4 #}</td>
<td>['0110', '0109', '0108', '0107', '0106', '0105', '0104', '0103', '0102', '0101', '0100']</td>
</tr>
<tr>
<td>MACRO1={{# fn.sequence 40, 43 #}</td>
<td>['43', '42', '41', '40']</td>
</tr>
<tr>
<td>{{fn.list_sort macro.MACRO1, D}}</td>
<td>['43', '42', '41', '40']</td>
</tr>
<tr>
<td>{{fn.list_sort macro.MACRO1, Descending}}</td>
<td>['0110', '0109', '0108', '0107', '0106', '0105', '0104', '0103', '0102', '0101', '0100']</td>
</tr>
<tr>
<td>MACRO5={{# fn.sequence 110, 108, 4 #}</td>
<td>['0108', '0109', '0110']</td>
</tr>
<tr>
<td>{{fn.list_sort macro.MACRO5, A}}</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>Output</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td><code>{{fn.one data.Countries. iso_country_code | emergency_access_ prefix:'112'}}}</code></td>
<td>A single result, e.g.</td>
</tr>
<tr>
<td></td>
<td>'FRA'</td>
</tr>
<tr>
<td></td>
<td>'abc'</td>
</tr>
<tr>
<td><code>{{fn.as_list data.Countries. country_name|country_name : 'Bahrain'}}}</code></td>
<td>['Bahrain']</td>
</tr>
<tr>
<td></td>
<td>['abc']</td>
</tr>
<tr>
<td><code>{{fn.list_empty}}</code></td>
<td>[]</td>
</tr>
<tr>
<td>MACRO1={{# fn.sequence 40, 43 #}}</td>
<td>['41','42']</td>
</tr>
<tr>
<td>MACRO2={{# fn.sequence 41, 42 #}}</td>
<td></td>
</tr>
<tr>
<td>(# fn.list_set_intersect macro.MACRO1, macro.MACRO2 #)</td>
<td></td>
</tr>
<tr>
<td>MACRO1={{# fn.sequence 40, 43 #}}</td>
<td>['40','41','42','43','44','45']</td>
</tr>
<tr>
<td>MACRO2={{# fn.sequence 41, 45 #}}</td>
<td></td>
</tr>
<tr>
<td>(# fn.list_set_left macro.MACRO1, macro.MACRO2 #)</td>
<td>['40']</td>
</tr>
<tr>
<td>MACRO1={{# fn.sequence 40, 43 #}}</td>
<td>['44','45']</td>
</tr>
<tr>
<td>MACRO2={{# fn.sequence 41, 45 #}}</td>
<td></td>
</tr>
<tr>
<td>(# fn.list_set_right macro.MACRO1, macro.MACRO2 #)</td>
<td></td>
</tr>
</tbody>
</table>

## Rule Filter Functions

The “filter by rule” function returns a list of resource instance data for a given model type. The schema of the model type in question must define a rules object of the form:

```json
'rules': {
```
The model `data/Role` is one example of such a model type. Filtering is applied using the current hierarchy context or else based on an explicit hierarchy type name.

Macro format:

```
{{ fn.filter_by_rule <rule name>,
  <model type>,
  <direction>,
  <attribute path to return>,
  <hierarchy type name> }}
```

Argument descriptions:

- `<rule name>`: The name of the rule being used to filter results. Supported values: `hierarchy_types`

- `<model type>`: The model type of the instances to be filtered.

- `<direction>`: The search direction of the results. Possible values are:
  - `all`: search at current hierarchy, ancestors, and descendants.
  - `up`: search at current hierarchy and ancestors.
  - `down`: search at current hierarchy and descendants.
  - `local`: search at current hierarchy only.

- `<attribute path to return>`: [optional] The path dot (.) delimited path to a single attribute to return
  - If not specified the returned result will contain a list of objects.
  - If specified the returned result will contain a list the given attribute.
  - Must be "null" if this field is not required, while `<hierarchy type name>` is supplied.

- `<hierarchy type name>`: [optional] The name of the hierarchy type to filter by. This will be looked up from the current hierarchy going up.

Examples:

```
{{ fn.filter_by_rule hierarchy_types, data/Role, up, name, Customer }}
```

Returns all the names of the roles that are permitted at "Customer" hierarchy type. Lookup is done from the current hierarchy upwards.

```
{{ fn.filter_by_rule hierarchy_types, data/Role, up, null, Customer }}
```

Returns full instance data of the roles that are permitted at "Customer" hierarchy type. Lookup is done from the current hierarchy upwards.

```
{{ fn.filter_by_rule hierarchy_types, data/Role, up, name }}
```

Returns all the names of the roles that are permitted at the hierarchy type of the current hierarchy context. Lookup is done from the current hierarchy upwards.

```
{{ fn.filter_by_rule hierarchy_types, data/Role, up }}
```

Returns full instance data of the roles that are permitted at the hierarchy type of the current hierarchy context. Lookup is done from the current hierarchy upwards.
Macro Function

- \textit{fn.evaluate}: Evaluate the string using the macro interpreter. The string can be a macro and can also contain macro names to be evaluated.

The function is so that we can save data as a macro and then evaluate it when we read it again.

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where self.x is:</td>
<td></td>
</tr>
<tr>
<td>{# data.Countries.iso_country_code</td>
<td></td>
</tr>
<tr>
<td>country_name:'South Africa' #}</td>
<td></td>
</tr>
<tr>
<td>Then:</td>
<td></td>
</tr>
<tr>
<td>{# fn.evaluate self.x #}</td>
<td></td>
</tr>
<tr>
<td>Where MACRO1 is:</td>
<td></td>
</tr>
<tr>
<td>{{ data.Countries.emergency_access_prefix</td>
<td></td>
</tr>
<tr>
<td>iso_country_code:FRA }}</td>
<td></td>
</tr>
<tr>
<td>Where MACRO2 is:</td>
<td></td>
</tr>
<tr>
<td>{# data.Countries.iso_country_code</td>
<td></td>
</tr>
<tr>
<td>emergency_access_prefix:macro.MACRO1 #}</td>
<td></td>
</tr>
<tr>
<td>Then:</td>
<td></td>
</tr>
<tr>
<td>{# fn.evaluate macro.MACRO2 #}</td>
<td></td>
</tr>
</tbody>
</table>

CUCM Functions

- \textit{fn.cucm_get_line_details}: Specify the line pattern and site name and use the Macro Evaluator function to view the line parameters for the specified line.

To return the result for a single line parameter, append the required parameter to the end of the macro
Subscriber Functions

- `fn.process_subscriber_line_data`: Used in workflows - a single parameter called input is the workflow input context, containing line data. The function returns line patterns and partitions found in any of Phone, DeviceProfile, RemoteDestinationProfile.

- `fn.process_subscriber_wizard_data`: Used in workflow CFT - a single parameter called input is the workflow input context, containing wizard data. The function returns Configuration Template data use for adding a relation/Subscriber instance.

Examples:

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
</table>
| {{ fn.cucm_get_line_details 4025, VS-Corp-NewYork }} | {
|     |     "is_line_shared": true,
|     |     "remote_destination_profiles": ["RDP_vdevenr"],
|     |     "device_profiles": ["UDP_vdevenr"],
|     |     "phones": ["SEP002155D547F7", "SEP111122223333"]
|     |   }
| {{ fn.cucm_get_line_details 4025, VS-Corp-NewYork, is_line_shared }} | true
| {{ fn.cucm_get_line_details 4025, VS-Corp-NewYork, phones }} | SEP002155D547F7
| | SEP111122223333 |

Examples:

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
</table>
| {{ fn.process_subscriber_line_data input }} | [{
|     |     "pattern": "10003",
|     |     "routePartitionName": "Site-23m-Customer 1 Site A"
|     | }, {
|     |     "pattern": "10005",
|     |     "routePartitionName": "Site-23m-Customer 1 Site A"
|     | }]

Cisco Unified Communications Domain Manager, Release 10.6(1) Maintain and Operate Guide
Example Configuration Template data snippet:
```
"data": {
  "description": "Template for provisioning a Subscriber from wizard using custom macro function",
  "name": "AddSubscriberWizard_CFT",
  "target_model_type": "relation/Subscriber",
  "template": "{{ fn.process_subscriber_wizard_data input }}"
}
```

### Zero, Unset and Boolean Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>fn.zero</td>
<td>Return a zero value.</td>
<td>{{fn.zero}}</td>
<td>0</td>
</tr>
<tr>
<td>fn.unset</td>
<td>Return an empty string.</td>
<td>{{fn.unset}}</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>fn.true</td>
<td>Return a boolean True.</td>
<td>{{fn.true}}</td>
<td>true</td>
</tr>
<tr>
<td>fn.false</td>
<td>Return a boolean False.</td>
<td>{{fn.false}}</td>
<td>false</td>
</tr>
</tbody>
</table>

### Time Functions

- **fn.now**: Return the date and time at this moment. An optional format parameter is available.

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>{{fn.now}}</td>
<td>2013-04-18 10:50:52.105130</td>
</tr>
<tr>
<td>{{fn.now &quot;%Y%m%d&quot;}}</td>
<td>20140327</td>
</tr>
<tr>
<td>macro.DAY=&quot;%A %m/%d/%Y&quot;</td>
<td>&quot;Thursday 03/27/2014&quot;</td>
</tr>
<tr>
<td>{{fn.now macro.DAY}}</td>
<td></td>
</tr>
</tbody>
</table>

Supported date and time formats

- `%a`: abbreviated weekday name according to the current locale
- `%A`: full weekday name according to the current locale
- `%b`: abbreviated month name according to the current locale
<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%B</td>
<td>full month name according to the current locale</td>
</tr>
<tr>
<td>%c</td>
<td>preferred date and time representation for the current locale</td>
</tr>
<tr>
<td>%C</td>
<td>century number (the year divided by 100 and truncated to an integer, range 00-99)</td>
</tr>
<tr>
<td>%d</td>
<td>day of the month as a decimal number (range 01 to 31)</td>
</tr>
<tr>
<td>%D</td>
<td>same as m/d/y</td>
</tr>
<tr>
<td>%e</td>
<td>day of the month as a decimal number, a single digit is preceded by a space (range '1' to '31')</td>
</tr>
<tr>
<td>%g</td>
<td>like G, but without the century</td>
</tr>
<tr>
<td>%G</td>
<td>The 4-digit year corresponding to the ISO week number</td>
</tr>
<tr>
<td>%h</td>
<td>same as b</td>
</tr>
<tr>
<td>%H</td>
<td>hour as a decimal number using a 24-hour clock (range 00 to 23)</td>
</tr>
<tr>
<td>%I</td>
<td>hour as a decimal number using a 12-hour clock (range 01 to 12)</td>
</tr>
<tr>
<td>%j</td>
<td>day of the year as a decimal number (range 001 to 366)</td>
</tr>
<tr>
<td>%m</td>
<td>month as a decimal number (range 01 to 12)</td>
</tr>
<tr>
<td>%M</td>
<td>minute as a decimal number</td>
</tr>
<tr>
<td>%n</td>
<td>newline character</td>
</tr>
<tr>
<td>%p</td>
<td>either 'AM' or 'PM' according to the given time value, or the corresponding strings for the current locale</td>
</tr>
<tr>
<td>%P</td>
<td>like p, but lower case</td>
</tr>
<tr>
<td>%r</td>
<td>time in a.m. and p.m. notation equal to I:M:S p</td>
</tr>
<tr>
<td>%R</td>
<td>time in 24 hour notation equal to H:M</td>
</tr>
<tr>
<td>%S</td>
<td>second as a decimal number</td>
</tr>
<tr>
<td>%t</td>
<td>tab character</td>
</tr>
<tr>
<td>%T</td>
<td>current time, equal to H:M:S</td>
</tr>
<tr>
<td>%u</td>
<td>weekday as a decimal number [1,7], with 1 representing Monday</td>
</tr>
<tr>
<td>%U</td>
<td>week number of the current year as a decimal number, starting with the first Sunday as the first day of the first week</td>
</tr>
</tbody>
</table>
%V  The ISO 8601:1988 week number of the current year as a decimal number, range 01 to 53, where week 1 is the first week that has at least 4 days in the current year, and with Monday as the first day of the week.

%w  day of the week as a decimal, Sunday being 0

%W  week number of the current year as a decimal number, starting with the first Monday as the first day of the first week

%x  preferred date representation for the current locale without the time

%X  preferred time representation for the current locale without the date

%y  year as a decimal number without a century (range 00 to 99)

%Y  year as a decimal number including the century

%z  numerical time zone representation

%Z  time zone name or abbreviation

%%  a literal '%' character

### Hierarchy Functions

- `fn.hierarchy` - Return the UUID of the current node.
- `fn.hierarchy_parent` - Return the UUID of the parent.
- `fn.hierarchy_path` - Return the current node hierarchy as a list of UUIDs.
- `fn.hierarchy_parent_path` - Return the current node parent hierarchy as a list of UUIDs.
- `fn.hierarchy_friendly_path` - Return the current node hierarchy as a dot-separated hierarchy string.
- `fn.hierarchy_friendly_parent_path` - Return the current node parent hierarchy as a dot-separated hierarchy string.

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>{{fn.hierarchy}}</td>
<td>'52162d552afa433946245bcb'</td>
</tr>
<tr>
<td>{{fn.hierarchy_parent}}</td>
<td>'52162d522afa433941245ba0'</td>
</tr>
</tbody>
</table>
### Request Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>fn.request_user_name</td>
<td>Return the logged-in username.</td>
<td>{{fn.request_user_name}}</td>
</tr>
<tr>
<td>fn.request_user_role</td>
<td>Return the logged-in user role.</td>
<td>{{fn.request_user_role}}</td>
</tr>
<tr>
<td>fn.request_user_email</td>
<td>Return the logged-in user email address</td>
<td>{{fn.request_user_email}}</td>
</tr>
<tr>
<td>fn.request_user_pkid</td>
<td>Return the logged-in user pkid.</td>
<td>{{fn.request_user_pkid}}</td>
</tr>
</tbody>
</table>

### Internal Number Inventory Functions

The `fn.lines` macro functions use the value of a `CUSTOMER_INI_ENABLED` macro at the relevant hierarchy:

- If `((True))`, then apply the function to the Internal Number Inventory at the hierarchy:
  
  ```
  data.InternalNumberInventory.internal_number.
  ```

- If `((False))`, then apply the function to `device.cucm.Line.pattern`, optionally with a specified `routePartitionName`. 

---

Cisco Unified Communications Domain Manager, Release 10.6(1) Maintain and Operate Guide
All macros will check the CUSTOMER_INI_ENABLED macro first. These macros exist at the required hierarchy level and have a value of (True) or (False).

- **CUSTOMER_INI_ENABLED macro is (False):**

Give the following patterns and route partition on the Unified Communications Manager:

<table>
<thead>
<tr>
<th>Number</th>
<th>Partition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td>Site-REL103-Customer</td>
</tr>
<tr>
<td>3000</td>
<td></td>
</tr>
<tr>
<td>4000</td>
<td>Site-REL103-Customer</td>
</tr>
<tr>
<td>5000</td>
<td>Site-REL103-Customer</td>
</tr>
<tr>
<td>6000</td>
<td></td>
</tr>
</tbody>
</table>

- **fn.lines** - Return a list of lines. With no parameter, list all the lines on the associated Unified Communications Manager. If the optional parameter is a route partition, list the lines in the partition. If the optional parameter is custom, show an empty list.

```
{{fn.lines}}

[{
"value": u'1000', "title": u'1000'},
{"value": u'2000', "title": u'2000'},
{"value": u'3000', "title": u'3000'},
{"value": u'4000', "title": u'4000'},
{"value": u'5000', "title": u'5000'},
{"value": u'6000', "title": u'6000'}]

{{fn.lines Site-REL103-Customer}}

[{
"value": u'2000', "title": u'2000'},
{"value": u'4000', "title": u'4000'},
{"value": u'5000', "title": u'5000'}]

{{fn.lines custom}}

[]
```

- **CUSTOMER_INI_ENABLED macro is (True):**

Given the following properties of an example Internal Number Inventory:
**Internal Number Inventory Functions**

<table>
<thead>
<tr>
<th>Number</th>
<th>In Use</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>2000</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>3000</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>4000</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>5000</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>6000</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

- **fn.lines** - Return a list of available lines on the Internal Number Inventory, with used lines indicated as (used).
- **fn.lines_available_only** - Return a list of available lines from the Internal Number Inventory, with <TITLE> in brackets.
- **fn.lines_used_only** - Return a list of used lines from the Internal Number Inventory, with <TITLE> in brackets after each.
- **fn.lines_unavailable_only** - Return a list of unavailable lines from the Internal Number Inventory, with <TITLE> in brackets after each.
- **fn.lines_unused_only** - Return a list of unused lines from the Internal Number Inventory, with <TITLE> in brackets after each.
- **fn.lines_available_used** - Return a list of available and used lines from the Internal Number Inventory, with <TITLE> in brackets after each.
- **fn.lines_available_unused** - Return a list of available and unused lines from the Internal Number Inventory, with <TITLE> in brackets after each.
- **fn.lines_unavailable_used** - Return a list of unavailable, used lines from the Internal Number Inventory, with <TITLE> in brackets after each.
- **fn.lines_unavailable_unused** - Return a list of unavailable and unused lines from the Number Inventory, with <TITLE> in brackets after each.

**Output Example**

```json
[{u'value': u'1000', u'title': u'1000'},
 {u'value': u'2000', u'title': u'2000'},
 {u'value': u'4000', u'title': u'4000 (used)'},
 {u'value': u'5000', u'title': u'5000 (used)'}]
```

---

Cisco Unified Communications Domain Manager, Release 10.6(1) Maintain and Operate Guide
Localization Functions

- **fn.localize** - Return a value that is localized, in other words it will be translated if a translation exists. It is used with a macro call that returns a value from a data store.

- **fn.list_installed_languages** - List the installed languages on the system. This includes languages in the administrator GUI and selfservice GUI.

---

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>{{fn.lines_available_only avail}}</td>
<td>[[u'value': u'1000', u'title': u'1000 (avail)'],</td>
</tr>
<tr>
<td></td>
<td>{u'value': u'2000', u'title': u'2000 (avail)'],</td>
</tr>
<tr>
<td></td>
<td>{u'value': u'4000', u'title': u'4000 (avail)'],</td>
</tr>
</tbody>
</table>
|                                              |    {u'value': u'5000', u'title': u'5000 (avail)']}
| {{fn.lines_used_only inuse}}                 | [[u'value': u'4000', u'title': u'4000 (inuse)'], |
|                                              |    {u'value': u'5000', u'title': u'5000 (inuse)']}
| {{fn.lines_unavailable_only}}                | [[u'value': u'3000', u'title': u'3000'], |
|                                              |    {u'value': u'6000', u'title': u'6000 (used)']}
| {{fn.lines_unused_only}}                     | [[u'value': u'1000', u'title': u'1000'], |
|                                              |    {u'value': u'2000', u'title': u'2000'], |
|                                              |    {u'value': u'3000', u'title': u'3000']}
| {{fn.lines_available_used}}                  | [[u'value': u'4000', u'title': u'4000 (used)'], |
|                                              |    {u'value': u'5000', u'title': u'5000 (used)']}
| {{fn.lines_available_unused}}                | [[u'value': u'1000', u'title': u'1000'], |
|                                              |    {u'value': u'2000', u'title': u'2000']}
| {{fn.lines_unavailable_used}}                | [[u'value': u'6000', u'title': u'6000']}
| {{fn.lines_unavailable_unused}}              | [[u'value': u'3000', u'title': u'3000']] |
Log Functions

- `fn.list_installed_languages_admin` - List the installed languages in the administrator GUI.
- `fn.list_installed_languages_selfservice` - List the installed languages in the selfservice GUI.
- `fn.list_installed_languages_by_role` - List the installed languages based on the User Role Interface value.

The User Role Interface value is a parameter of this function:

- `admin` - installed languages in the admin GUI
- `self-service` - selfservice GUI
- `none` - union of admin and selfservice languages

### Example

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>```{{fn.localize data.LocalizedModelStore.localized_value</td>
<td>where_clause}}```</td>
</tr>
<tr>
<td><code>#{fn.list_installed_languages #}</code></td>
<td><code>[{'value': 'en-us', 'title': 'English'},{'value': 'de-de', 'title': 'German'}]</code></td>
</tr>
<tr>
<td><code>#{fn.list_installed_languages_admin #}</code></td>
<td><code>[{value': 'en-us', 'title': 'English'}]</code></td>
</tr>
<tr>
<td><code>#{fn.list_installed_languages_selfservice #}</code></td>
<td><code>[{value': 'en-us', 'title': 'English'}, {value': 'de-de', 'title': 'German'}]</code></td>
</tr>
<tr>
<td><code>#{fn.list_installed_languages_by_role none #}</code></td>
<td><code>[{value': 'en-us', 'title': 'English'}, {value': 'de-de', 'title': 'German'}]</code></td>
</tr>
</tbody>
</table>

### Log Functions

- `fn.log` - Given a log level and message, display it in the log. Log levels can be: debug, critical, warn, error or info.
- `fn.txn_log` - Given a message, display it in the transaction log on the GUI.

The macro is typically added to a workflow "Set" step for debugging purposes.

### Example

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{{fn.log info, This is an informational message.}}</code></td>
<td><strong>In app.log:</strong></td>
</tr>
<tr>
<td><code>{{fn.log debug, Debug message.}}</code></td>
<td>INFO This is an informational message.</td>
</tr>
<tr>
<td></td>
<td>DEBUG Debug message.</td>
</tr>
</tbody>
</table>
**Object Keys Functions**

Example object:

```
{  
  "input": {  
    "object": {  
      "boolean_1": true,  
      "boolean_2": false,  
      "boolean_3": true,  
      "string_1": "1",  
      "string_1_dup": "1",  
      "string_2": "2",  
      "integer_1": 1,  
      "integer_1_dup": 1,  
      "integer_2": 2  
    }  
  }  
}
```

- `fn.object_keys` - Given an object and additional optional parameter, return the list of keys that match the parameter value, or all the keys if no parameter value is given.

Examples:

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{ fn.object_keys input.object,true }</code></td>
<td>[&quot;boolean_1&quot;,&quot;boolean_3&quot;]</td>
</tr>
<tr>
<td><code>{fn.object_keys input.object,&quot;1&quot;}</code></td>
<td>[&quot;string_1&quot;,&quot;string_1_dup&quot;]</td>
</tr>
<tr>
<td><code>{fn.object_keys input.object,1}</code></td>
<td>[&quot;integer_1&quot;,&quot;integer_1_dup&quot;]</td>
</tr>
<tr>
<td><code>{fn.object_keys input.object}</code></td>
<td>[&quot;boolean_1&quot;,&quot;boolean_2&quot;,&quot;boolean_3&quot;, &quot;string_1&quot;,&quot;string_1_dup&quot;,&quot;string_2&quot;, &quot;integer_1&quot;,&quot;integer_1_dup&quot;,&quot;integer_2&quot;]</td>
</tr>
</tbody>
</table>
Macro and Macro Function Nesting

Macros and macro functions can be used as arguments of macros and macro functions. Consider the examples below:

1. Define a macro Masklen as `{{fn.length This is a valid string}}`.
2. Define a macro as `{{fn.mask X macro.Masklen 0}}`.
3. The result is evaluated as 'XXX...' to the length of 'This is a valid string'.

Conversion Functions

- **fn.pkid_to_bkey** - Given a pkid, return the business key.
- **fn.bkey_to_pkid** - Given a business key, return the pkid. Provide the data type as an argument.
- **fn.as_int** - Given a string, return an integer
- **fn.as_string** - Given an integer, return a string.
- **fn.as_list** - Given input, return it as a list. List input is returned as is.

Examples:

<table>
<thead>
<tr>
<th>Example</th>
<th>Output</th>
</tr>
</thead>
</table>
| macro: USA_pkid = {{data.Countries.__pkid|iso_country_code:USA}}
{{fn.pkid_to_bkey macro.USA_pkid}} | "[u'United States of America', u'USA', u'']" |
| macro: a_country_bkey =
{{data.Countries.__bkey\__pkid:macro.USA_pkid}}
{{fn.bkey_to_pkid macro.a_country_bkey, data/Countries}} | "52d3eba8893d57373f842acb" |
| {{fn.as_int "1"}} | 1 |
| {{fn.as_string 12345}} | "12345" |
| {{fn.as_bool "T"}} | true |
| {{fn.as_bool "0"}} | false |
Conditional Logic Macro Function

Conditional logic in macros is supported by the `fn.conditional_logic` function that takes two parameters:

- the name of an instance of the `data/ConditionalLogic` data model.
- a value that serves as input to the `data/ConditionalLogic` data model.

The namespaces that can be used as `left_expression` values in the data model can depend on the reference to the data model in a Provisioning Workflow. The namespaces - that can also be referenced in full - include:

- `{{self}}`
- `{{previous}}`
- `{{input}}`
- `{{cft}}`
- `{{pwf}}`

Consider the following example `data/ConditionalLogic` data model called "Is_SLC_Allowed":

```json
"conditions": [
    {
        "unary_operator": "NOT",
        "right_expression": "{{ logic.DATA }}",
        "conditional_operator": "AND",
        "condition": "contains",
        "left_expression": "{{ pwf.SLCS }}"
    },
    {
        "unary_operator": "NOT",
        "right_expression": "{{ input.CURRENT_SLC }}",
        "conditional_operator": "AND",
        "condition": "containsStartOf",
        "left_expression": "{{ logic.DATA }}"
    },
    {
        "right_expression": "{{ input.CURRENT_SLC }}",
        "condition": "containsStartsWith",
        "unary_operator": "NOT",
        "left_expression": "{{ logic.DATA }}"
    }
]
```

Also suppose the Provisioning Workflow for this example has a list variable `SLCS` and receives an `input.CURRENT_SLC` value.

Furthermore, during the call of the `fn.conditional_logic` function in the Provisioning Workflow, it receives a scalar value as an argument, for example:

```json
{{ fn.conditional_logic Is_SLC_Allowed, 128 }}
```
• The scalar value reference {{ logic.DATA }} can be omitted from either left_expression or right_expression. Its reference is then assumed.

• The input value is referenced as {{ input.CURRENT_SLC }}

• The list that is the Provisioning Workflow variable, is {{ pwf.SLCS }}

As another example, consider a data/ConditionalLogic model called “TestData” with three conditions:

```
"conditions": [  
  {  
    "conditional_operator": "OR",
    "left_expression": "{{input.DATA}}",
    "condition": "contains",
    "right_expression": "AAA"
  },  
  {  
    "conditional_operator": "AND",
    "left_expression": "{{input.DATA}}",
    "condition": "contains",
    "right_expression": "BBB"
  },  
  {  
    "left_expression": "{{input.DATA}}",
    "condition": "contains",
    "right_expression": "CCC",
    "unary_operator": "NOT"
  }
]
```

The following function checks if a received input value “AAAaaaBBBaaaCCc” fulfills the condition: contains “AAA” OR “BBB” AND NOT “CCC”, as in the macro test using a scalar value:

```
{{ fn.conditional_logic TestData, AaaaBBBaaaCCc }}
```

The condition resolves to true.

Finally in the following example, the conditional function is used as a condition in a Provisioning Workflow. The Data Model instance of data/ConditionalLogic called "Does Newland Exist" tests a single string matching condition:

```
"data": {  
  "conditions": [  
    {  
      "right_expression": "Newland",
      "condition": "is exactly",
      "left_expression": "{{pwf.EXIST}}"
    }
  ],  
  "name": "Does Newland Exist"
}
```

The Provisioning Workflow step to apply a Configuration Template if the condition is false. So the step is carried out only if there is not already a country_name called "Newland".

```
"workflow": [  
  {  
    "templates": [  
      {  
        "conditions": [  
          {  
            "condition": "( fn.conditional_logic "Does Newland Exist" == False )"
          }
        ],  
        "template": "CFT1"
      }
    ],  
    "entity": "data/Countries",
    "set_list": [  
      {  
        "set_var_name": "EXIST",
        "set_var_value": "{{data.Countries.country_name|country_name:Newland}}"
      }
    ]
  }
]"## Conditional Logic Macro Function

Cisco Unified Communications Domain Manager, Release 10.6(1) Maintain and Operate Guide

332
HTTP GET Function

- `fn.request_get` - Return in JSON format the response of an HTTP request. The HTTP request must start with `http://localhost`.

Example request:

```plaintext
{{ fn.request_get http://localhost/api/data/Countries/properties }}
```

The output can be assigned to a variable so that properties can be referenced.

Example with output snippet:

```plaintext
http://localhost/api/data/Countries/properties
{
  "meta": {
    "query": "/api/data/Countries/properties/?hierarchy=[hierarchy]&format=json"
  },
  "choices": [ ]
}
```

Example of instance output with GET request for an instance with `{pkid}`:

```plaintext
http://localhost/api/data/Countries/54e1de60edec65160652e402
{
  "business_key": {
    "hierarchy": true,
    "unique": {
      "country_name",
      "iso_country_code"
    }
  },
  "tagged_versions": [],
  "data": {
    "iso_country_code": "MEX",
    "pstn_access_prefix": "9",
    "pkid": "54e1de60edec65160652e403",
    "default_user_locale": "English United States",
    "network_locale": "United States",
    "standard_access_prefix": "0",
    "international_access_prefix": "00",
    "country_name": "Mexico",
    "international_dial_code": "52",
    "emergency_access_prefix": "066",
    "national_trunk_prefix": "01"
  }
}
```
Macro Examples Simple

Simple macros must always resolve to one value only.

```python
{{data.Countries.iso_country_code | country_name:'South Africa'}}
'ZAF'
```

Call to a non-existent macro.

```python
{{macro.DoesNotExist}}
{u'code': 6003,
 u'http_code': 400,
 u'message': u'Macro lookup of macro.DoesNotExist failed at hierarchy sys',
 u'transaction': None}
```

First Partition member name in CSS PSTN-CSS-Cape-Town.

```python
{{ device.cucm.Css.members.member.0.routePartitionName | name: 'PSTN-CSS-Cape-Town' }}
'PHONES-PT-Cape-Town'
```

First Partition member UUID in CSS PSTN-CSS-Cape-Town.

```python
{{ device.cucm.Css.members.member.0.uuid | name: 'PSTN-CSS-Cape-Town' }}
'(7AF255DC-3A05-A1B4-9E5E-95CD48C3C95F)'
```

Macro Examples List Macro

Syntax for List macros is between `{##}`. The results are in a list format: comma-separated results and between [] All fields in Countries model.

```python
#{ data.Countries.* #}
[{u'cli_on_prefix': u'',
  u'country_name': u'Australia',
  u'data_type_': u'data/Countries',
  u'default_user_locale': u'English United States',
  u'emergency_access_prefix': u'000',
  u'international_access_prefix': u'011',
  u'international_dial_code': u'61',
  u'iso_country_code': u'AUS',
  u'network_locale': u'United States',
  u'premium_access_prefix': u'8',
  u'pstn_access_prefix': u'9',
  u'service_access_prefix': u'13'},
  {u'cli_on_prefix': u'',
  u'country_name': u'Bahrain',
  u'data_type_': u'data/Countries',
  u'default_user_locale': u'English United States',
  u'emergency_access_prefix': u'999',
  u'international_access_prefix': u'00',
  u'international_dial_code': u'973',
  u'iso_country_code': u'BHR',
  u'network_locale': u'United States',
  u'premium_access_prefix': u'',
  u'pstn_access_prefix': u'9',
  u'service_access_prefix': u''}],
```

Selected fields in Countries model.

```python
#{ data.Countries.country_name, iso_country_code #}
[{u'country_name': u'Australia',
  u'iso_country_code': u'AUS'},
  {u'country_name': u'Bahrain',
  u'iso_country_code': u'BHR'},
  {u'country_name': u'Canada',
  u'iso_country_code': u'CAN'},
  {u'country_name': u'Denmark',
  u'iso_country_code': u'DNK'}]
Specifying one field in the list will return only a list of values and not a key-value pair list.

```python
{u'iso_country_code': u'USA', u'country_name': u'United States of America'}
```

Device types: a list of all line patterns in the null partition.

```python
{u'routePartitionName': u'NullPartition', u'pattern': u'55554444', u'routePartitionName': u'NullPartition', u'pattern': u'8100240105', u'routePartitionName': u'NullPartition', u'pattern': u'5544332211', u'routePartitionName': u'NullPartition', u'pattern': u'56667722', u'routePartitionName': u'NullPartition', u'pattern': u'8765653', u'routePartitionName': u'NullPartition', u'pattern': u'66776767', u'routePartitionName': u'NullPartition', u'pattern': u'3009', u'routePartitionName': u'NullPartition', u'pattern': u'656574747', u'routePartitionName': u'NullPartition'}
```

Nested structures.

```python
{u'member': [{u'index': 1, u'routePartitionName': u'PHONES-PT-Cape-Town', u'uuid': u'7AF255DC-3A05-A1B4-9E5E-95CD48C3C95F'}, {u'index': 2, u'routePartitionName': u'PSTN-PT-Cape-Town', u'uuid': u'5FA76732-0074-108A-3A91-23D7C6CAC2E1'}, {u'index': 3, u'routePartitionName': u'PSTN-PT-Cape-Town', u'uuid': u'F789964F-C95D-4095-F6C7-48E587CBFA9D'}, {u'index': 4, u'routePartitionName': u'CallPark-PT-Cape-Town', u'uuid': u'B4817113-0F32-6E7F-67B2-20645CFC4509'}], u'name': u'PSTN-CSS-Cape-Town', u'hierarchy': u'5170100ec2619483c1291b', u'members': [{u'index': 1, u'routePartitionName': u'PHONES-PT-Cape-Town', u'uuid': u'7AF255DC-3A05-A1B4-9E5E-95CD48C3C95F'}], u'partitionUsage': u'General', u'name': u'PSTN-CSS-Cape-Town', u'uuid': u'{E678A23E-866A-7CE8-AD0F-8AF138E10A18}'}
```
Create a Macro In-line

To create a macro in-line, enter the macro directly in:

1. Default value in a Data Model.
2. Default value in a Configuration Template.
3. Condition of an Operation in a Provisioning Workflow.

Create a Value Substitution Macro

To write a value substitution macro:

1. Determine where to enter the macro: in-line or for re-use.
2. Determine the reference of the value to resolve:
   • Data Model reference syntax is "data/datamodel.attribute" or "datamodel.attribute". The first instance of the datamodel.attribute will be the target.
   • Syntax for a reference to an attribute in a Domain Model is "self.attribute"
3. Enter any static text that should combine with the evaluated macro - if required. Static text is entered outside the "{{" and "}}".

Substitution Macro Examples

```
{{CallManager.host}}
http://{{CallManager.host}}
http://{{CallManager.host}}/{{CallManager.username}}:
```
Create an Evaluation Macro

To write an evaluation macro:

1. Identify tests and result values:
   - A simple test resolves to True or False.
   - An If-Then-Else test resolves to a value.

2. For a simple test, identify the values and operator to resolve to True or False.

3. For an If-Then-Else test, identify If-, Else- and default conditions and values.

Evaluation Macro Examples

(((DATA1.d1 == y)))
Explanation: this macro evaluates to true if DATA1.d1 is equal to y.

(((EVALUATE1.val == y)) <{CallManager.host}-Enabled> ((EVALUATE1.val == n)) <{CallManager.host}-Disabled> <{CallManager.host}-Not set>

Explanation: this macro evaluates data model called “EVALUATE1” with attribute “val” - to value of data model called “CallManager” and with attribute “host”:

- Appended with “-Enabled” if EVALUATE1.val is y
- Appended with “-Disabled” if EVALUATE1.val is n
- Otherwise appended with “-Not set”
SNMP

- Introduction to SNMP and MIB, page 339
- SNMP Traps, page 341
- Management Information Bases, page 343
- MIB and Trap Details, page 344

Introduction to SNMP and MIB

Simple Network Management Protocol (SNMP) is a UDP-based network protocol used mostly in network management systems to monitor network-attached devices. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF) and consists of a set of standards for network management, including an application layer protocol, a database schema and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems that describe the system configuration. These variables can be queried using SNMP management applications.

SNMP allows a Network Management Station to do the following:

- Poll a device for info or to trend data i.e. Cisco Unified Communications Domain Manager 10.6(1) server load graph via HOST-SYSTEMS-MIB
- Receive notifications in the form of traps or informs in response to events, threshold violations, whatever the trap definitions in the loaded MIBs are. We enable process monitoring and disk space checks - when triggered, these send out a trap.

A management information base (MIB) is a form of virtual database used for managing the entities in a communications network. Working closely with SNMP, the hierarchical data structure describes all of the objects that a device can report the status of.

The MIB is structured based on the RFC 1155 standard. This standard defines how the MIB information is organized, what data types are allowed and how resources within the MIB are named. Each MIB contains the name, object identifier (a numeral), data type and the permissions relating to whether the value can be read or written to. The top hierarchies of the MIB are fixed; however, certain sub trees can be defined by product vendors and other organizations.

The variables within MIB are named using the Abstract Syntax Notation 1 (ASN.1). This is an international standard for representing data.
SNMP Terminology:

• MIB: The term MIB is used to refer to the complete collection of management information available on an entity, while MIB subsets are referred to as MIB-modules.

• NMS: A Network Management System is a combination of hardware and software used to monitor and administer a network and the devices associated with that network.

Configuration

SNMP on Cisco Unified Communications Domain Manager 10.6(1) is configured after initial system setup. The following SNMP parameters can be configured.

• SNMP integration
  Enable SNMP functionality. If this setting is disabled, the other SNMP parameters will not be displayed for configuration.

• SNMP system name
  The SNMP system name identifies the system being monitored on the NMS (Network Management System). Defaults to nodename.domainname.

• SNMP system location
  The SNMP system location describes the location of the system. Defaults to Unknown.

• SNMP system contact
  The SNMP system contact defines the email address of administrator responsible for the system. Defaults to None.

• SNMP query source
  CIDR-style IP (e.g. 196.0.0.0/8) network allowed to query SNMP from this host. This is used to limit the hosts allowed to manage the system via SNMP. Defaults to all hosts.

• SNMP load triggers
  The 1, 5 and 15 minute load averages that will trigger warnings via SNMP. Defaults to values dynamically calculated from the number of CPUs in the system. This should be formatted as 8n/4n/2n (where n represents the number of processors available) when entered into the configuration wizard during setup.

• SNMP trap destination
  This is the destination to which SNMP traps will be sent. Formatted as destination[community[port]] where both community and port are optional, but port may not be specified unless community is specified too.

• SNMP inform destination
  Inform events are similar to traps, except that they are acknowledged at the network layer to ensure delivery of the event notification. Formatted as destination[community[port]] where both community and port are optional, but port may not be specified unless community is specified too. It is generally preferable that SNMPv2 trap destinations are used instead, while leaving this field blank.
SNMP Traps

When the managed system generates certain events, it will forward a SNMP trap. The reason for the event trap is contained in the SNMP MIB string. Note that if the corresponding SNMP MIB is not loaded on the NMS, a numerical representation of the SNMP entry is provided. The list of monitored events is described in the SNMP Trap section below. A detailed breakdown of each SNMP trap type is provided in the appendix.

The SNMP will send traps to the trap destination configured. If the trap destination is incorrect or not configured, the NMS will not receive the traps.

The following system parameters are monitored by default:

- Disk Space: warnings are issued if the file system becomes full
- System Load Monitoring: warnings are issued if the system load is excessive (the system load parameters can be defined during configuration)
- SNMP: standard SNMP System Events, for example, Cold Start
- Process state changes: Informative messages are sent to the NMS indicating that processes have been restarted.

In general, the originator of the SNMP traps is determined by originating hostname / IP address. Many Network Management Systems provide trap management and escalation per system being managed, including identification based on system name, location and contact details. Those events monitored directly by Cisco Unified Communications Domain Manager 10.6(1) (e.g. disk space, system load and process warnings) include the system name as part of the variable bindings to assist identification of the originating system.

Disk Space Low [High Priority]

- Priority: HIGH
- Action: Call support

SNMP monitors the percentage of free space available, and will raise a trap if the filesystem becomes full. By default, the threshold is 10% free space available. The filesystem is used to store log files, etc. and under normal conditions will recycle these to ensure that disk space is managed. If a disk space low warning is received, it should be treated as a high priority, customer support should be contacted to determine the reason for the filesystem becoming full.

Excessive Load [Medium Priority]

- Priority: Medium
- Action: Monitor for short-term spikes (e.g. 1 and 5 minute intervals)
- Action: Escalate to support if excessive load average reported over 15 minute intervals.

During configuration, the maximum load can be specified as an average over 1 minute, 5 minute and 15 minute intervals. The system load may spike during certain activities such as bulk loading and will recover. The warning should only be treated as serious if the system load is high for an extended period (e.g. over a 10 minute average).

The load can be monitored either on the NMS for further excessive load traps, or via the command line interface (documented in the Command line interface guide) using the status and healthlog commands.
If the 15-minute threshold is exceeded, diagnosis is required to determine the cause of the high load. Ensure that sufficient CPU and Memory resources are available to the Cisco Unified Communications Domain Manager 10.6(1) system as per the initial hardware scaling requirements. The problem may also be caused by incidents such as network outages, delayed backups, manual intervention by a system administration, etc. Please contact support for further diagnosis of the problem.

Process State Changes [Medium Priority]

- **Priority:** Medium
- **Action:** Monitor

Process state changes (e.g., restart of services) are normal behavior when the Cisco Unified Communications Domain Manager 10.6(1) system is started or shutdown. Manual intervention by a system administrator is also likely to cause services to start or stop. The system manages processes automatically and will restart services as required. Process state changes are normal during HA (cluster failover).

The state of processes can be monitored either on the NMS for subsequent process state change traps, or via the command line interface (documented in the Command line interface guide) using the monitor command.

Check if there is a known outage, change control window, or scheduled work in progress for this platform. If there is none, then these traps represent a high priority issue and need to be logged with support.

Standard SNMP Events [Low Priority]

- **Priority:** Low
- **Action:** Monitor

Standard SNMP traps for cold-start and shutdown are generated by the Cisco Unified Communications Domain Manager 10.6(1) system when it is started or shutdown. Manual intervention by a system administrator may also generate these traps if the system is restarted. Cold-start notices may also indicate HA (cluster failover).

The state of the Cisco Unified Communications Domain Manager 10.6(1) system can be monitored either on the NMS for subsequent cold-start traps, or via the command line interface (CLI) using the monitor and healthlog commands.

Check if there is a known outage, change control window, or scheduled work in progress for this platform. If there is none, then these traps represent a high priority issue and need to be logged with support.

Reconfigure SNMP

SNMP configuration settings can be managed from the CLI. Refer to the CLI `notify` command:

```
platform@development:~$ notify
USAGE:
=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=0

```

SNMP URI usage:

- `snmpv2`: `snmp://community@host[:port]`
- `snmpv3`: `snmp://user:auth:password}@host[:port]` ... minimum auth/password length is 8 characters.

For example:

- `snmpv2`: `notify add info snmp://public@1.2.3.4`
• snmpv3: notify add snmp://public:publicauth:password@1.2.3.4

The following options can be configured under the SNMP menu in the CLI.
• Enabled - Enable or disable SNMP Queries
• Community - SNMP v2c Community String used to query this server
• Authorized Username - SNMP v3 Username to query this server
• Password - SNMP v3 Password to query this server
• Query - IP address that is allowed to query this server
• Sysname - Name of this server, as it will appear when queried via SNMP
• Syslocation - Location of this server
• Syscontact - Contact person(s) for this server (email address)
• Load1 - 1 Minute load average alarm value
• Load5 - 5 Minute load average alarm value
• Load15 - 15 Minute load average alarm value

Two SNMP Trap destinations can be configured:
The following options can be configured in the CLI:
• Hostname - Server name to send SNMP traps to.
• Version - Version of SNMP to use for sending trap, version 2c or 3.
• Community - refer to the SNMP-URI command usage.
• Mode - Send Trap or Inform message.
• Username - refer to the SNMP-URI command usage.
• Password - refer to the SNMP-URI command usage.
• Encryption - refer to the SNMP-URI command usage.
• Engineid - To send traps as. - Currently not implemented

Management Information Bases

SNMP information is grouped together in Management Information Bases (MIBs). The MIBs loaded on the Cisco Unified Communications Domain Manager 10.6(1) system represent all the configuration/data items that can be queried or be used to generate traps (notifications) when certain events occur. A list of all MIBs loaded on the system is provided below.

In order to manage the system, a Network Management System (NMS) should be installed at the customer site (e.g. HP OpenView, iReasoningMib Browser). The NMS should be loaded with the same set of MIBs as those installed on the system. The NMS should be configured to send SNMP queries to the managed host (i.e. correct IP address, port number (default 161), community string (default public), and version (default version 2c). Further, the NMS should be configured to receive traps from the managed host - the correct IP, port number (default 162), version (default version 2), and community strings (default public) should be provided).
SNMP items can be selected in the MIBs and the item queried on the remote managed system. The remote system will return a response to the MIB entry being queried. For example, if the following entry is queried (.1.3.6.1.2.1.1.5.0 alias .iso.org.dod.internet.mgmt.mib-2.system.sysName.0), the system will return the system name that was assigned during setup (e.g. sysName.0 'Voss Node00'). Note that if any of the configured details on the NMS are incorrect, it is likely that the query will never reach the managed host and no response will be received. Please ensure that version 2 is selected with the correct community string (default public).

When the managed system generates certain events, it will forward a SNMP trap. The reason for the event trap is contained in the SNMP MIB string. Note that if the corresponding SNMP MIB is not loaded on the NMS, a numerical representation of the SNMP entry is provided. The list of monitored events is described in the SNMP Trap section below.

Refer to the MIB List at the end of this document for the list of net-SNMP packages that ship with Cisco Unified Communications Domain Manager 10.6(1).

MIB and Trap Details

**SNMPv2-MIB - RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)**

Basic information about SNMP on the entity. Includes:

- sysDescr: A text description of the entity
- sysObjectID: The vendor's authoritative identification of the network management subsystem contained in the entity.
- sysUpTime: The time since the network management portion of the system was last re-initialised.

Note

sysUpTime indicates how long the SNMP software has been running on the box, and not how long the box itself has been up (this is a common misconception).

- Counters for SNMP requests and responses.

**IF-MIB - RFC 2863 - The Interfaces Group MIB**

Describes the network interfaces on the entity. For each interface the following information is given:

- ifType: The type of interface
- ifMtu: Size of the largest packet which can be sent/received on the interface
- ifSpeed: An estimate of the interface's current bandwidth
- ifPhysAddress: The interface’s address at its protocol sub-layer. For 802.x interfaces, this is the MAC address
- The administrative and operational state of the interface
• The number of octets and packets sent and received on the interface

MIB-II - RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets

TCP/IP network information not covered by the other MIBs, split into a number of groups:
• Address translation group:
  • atPhysAddress: The media-dependent physical address
  • atNetAddress: The network address (IP address) corresponding to the physical address
• IP group:
  • ipRouteTable: IP routing table, contains an entry for each route presently known to this entity

IP-MIB - RFC 4293 - Management Information Base for the Internet Protocol (IP)

Internet Protocol information:
• Counters for IP packets sent and received
• For each IP address:
  • The IP address
  • Index of the physical interface (in the IF-MIB)
  • Netmask
  • ICMP counters

TCP-MIB - RFC 4022 - Management Information Base for the Transmission Control Protocol (TCP)

TCP information:
• Retransmission timeout information
• Overall counters for number of inbound and outbound connections
• For each current connection:
  • Connection state
  • Local and remote IP addresses and TCP port numbers
UDP-MIB - RFC 4113 - Management Information Base for the User Datagram Protocol (UDP)

UDP information:
- Counters for datagrams sent and received
- Local IP addresses and UDP port numbers

HOST-RESOURCES-MIB - RFC 2790 - Management Information Base for Host Resources

Objects useful for the management of host computers. These are split into a number of groups:

- System Group
  - hrSystemUptime: Amount of time since the host was last initialized (note this is different from sysUpTime).
  - hrSystemDate: The host’s notion of the local date and time of day
  - hrSystemProcesses: The number of process contexts currently loaded or running on this system

- Storage Group
  - hrMemorySize: The amount of physical read-write main memory, typically RAM, contained by the host
  - For each storage device:
    - hrStorageType: The type of storage (RAM, fixed disk etc.)
    - hrStorageDescr: A description of the storage (Swap Space, mount point etc.)
    - Size of storage units, number available and number used

- Device Group
  - For each device:
    - Type (processor, network, disk, printer etc.)
    - Description
  - For each disk storage device:
    - Access (read-write, read-only)
    - Fixed/removable
    - Capacity
  - For each disk partition:
• Label
  • For each file system:
    • Mount point
    • Type
    • Access (read-write, read-only)
    • Bootable

• Running Software Group
  • For each running process:
    • Name
    • Path
    • Parameters
    • Status

• Running Software Performance Group for each running process:
  • CPU resources consumed by this process
  • Amount of real system memory allocated to this process

**SNMP Traps: System Startup**

**Identification**
• The originating IP / hostname is used to identify the system generating the traps
• The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
• alarms and escalation to the relevant system operator
• .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.coldStart

**Trap OID**
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.coldStart

**Variable Bindings**
• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 190 milliseconds (19)
• snmpTrapOID = coldStart
• .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapEnterprise.0 = linux
SNMP Traps: Service Startup Changes Made

The following events are generated at startup indicative of the various services changing state:

SNMP 1.3.6.1.2.1.88.2.0.1
2014-07-04 15:40:30 <server_IP> [UDP: [<server_IP>]:56005->[<snmp_server_IP>]]:
  iso.3.6.1.2.1.1.3.0 = Timeticks: (8785393) 1 day, 0:24:13.93 iso.3.6.1.6.3.1.1.4.1.0 = OID:
  iso.3.6.1.2.1.88.2.0.1 iso.3.6.1.2.1.88.2.1.1.0 = STRING: "ProcessRestart"
  iso.3.6.1.2.1.88.2.1.3.0 = STRING: <resource> iso.3.6.1.2.1.88.2.1.5.0 = INTEGER: 1 iso.3.6.1.2.1.1.5.0 = STRING:
  "<hostname>

where<resource> is one of the following:

- voss-deviceapi:voss-wsgi
- voss-deviceapi:voss-notifications
- voss-deviceapi:voss-queue
- mongodb:router
- mongodb:config
- mongodb:arbiter
- mongodb:database
- snmp:daemon
- snmp:traps
- nginx:proxy
- services:wsgi
- services:logs
- services:firewall
- services:mount
- services:time
- services:syslog

SNMP Traps: Service Monitoring - Changes Made

For each of the services listed above, the system will monitor the process and restart as necessary.

When the service shuts down, it sends a trap indicating a resource stopped in the following format:

2014-07-04 15:40:30 <server_IP> [UDP: [<server_IP>]:56005->[<snmp_server_IP>]]:
  iso.3.6.1.2.1.1.3.0 = Timeticks: (8785393) 1 day, 0:24:13.93 iso.3.6.1.6.3.1.1.4.1.0 = OID:
  iso.3.6.1.2.1.88.2.0.1 iso.3.6.1.2.1.88.2.1.1.0 = STRING: "ProcessStop"
  iso.3.6.1.2.1.88.2.1.3.0 = STRING: <resource> iso.3.6.1.2.1.88.2.1.5.0 = INTEGER: 1 iso.3.6.1.2.1.1.5.0 = STRING:
  "<hostname>"
Service restart is indicated by the following:

```
2014-07-04 15:40:30 <server_IP> [UDP: [server_IP]:56005->[snmp_server_IP]]:
iso.3.6.1.2.1.1.3.0 = Timeticks: (8785393) 1 day, 0:24:13.93
iso.3.6.1.2.1.88.2.0.1 iso.3.6.1.2.1.88.2.1.1.0 = STRING: "ProcessRestart"
iso.3.6.1.2.1.88.2.1.3.0 = STRING: <resource>
iso.3.6.1.2.1.88.2.1.5.0 = INTEGER: 1
iso.3.6.1.2.1.1.5.0 = STRING: "<hostname>
```

### SNMP Traps: System Shutdown

#### Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator

#### Trap OID

```
.iso.org.dod.internet.private.enterprises.netSnmp.netSnmpNotificationPrefix.netSnmpNotifications.nsNotifyShutdown
```

#### Variable Bindings

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 44 seconds (4414) snmpTrapOID = nsNotifyShutdown
.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapEnterprise.0
= netSnmpNotificationPrefix
```

### SNMP Trap: Disk Full

#### Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`
- The following variable binding can be used to determine that a disk partition is full.
disman-EventMIBNotificationObjects.mteHotTrigger.0 = ERROR: Disk full`
• The following variable binding can be used to further diagnose the extent of the filesystem that has become full
  • .iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskErrorMsg.1 = /: less than 75% free (= 26%)

Trap OID


Variable Bindings

• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
• snmpTrapOID = mteTriggerFired
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTargetName.0 =
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotContextName.0 =
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotOID.0 = dskErrorFlag.1
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1
• .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
• .iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskPath.1 = /
• .iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskErrorMsg.1 = /: less than 75% free (= 26%)

SNMP Trap: Excessive Load

Identification

• The originating IP / hostname is used to identify the system generating the traps
• The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
• The trap OID is generic for various SNMP events monitored by the system
• The SNMP system name is included as part of the variable binding to assist identification:
  • .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
• The following variable binding can be used to determine that the load average threshold has been exceeded.


• The following variable binding can be used to further diagnose which time interval threshold has been exceeded.

   - iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry.laNames.<LoadIdx> = <LoadError>
   - iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry.laErrMessage.<LoadIdx> = <LoadMessage>

<table>
<thead>
<tr>
<th>Load average interval</th>
<th>&lt;LoadIdx&gt;</th>
<th>&lt;LoadError&gt;</th>
<th>&lt;LoadMessage&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 minute</td>
<td>1</td>
<td>Load-1</td>
<td>1 min Load Average too high (= 2.52)</td>
</tr>
<tr>
<td>5 minute</td>
<td>2</td>
<td>Load-5</td>
<td>5 min Load Average too high (= 1.27)</td>
</tr>
<tr>
<td>15 minute</td>
<td>3</td>
<td>Load-15</td>
<td>15 min Load Average too high (= 1.27)</td>
</tr>
</tbody>
</table>

**Trap OID**


**Variable Bindings**

- iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationObjects.mteHotTargetName.0 =
- iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationObjects.mteHotContextName.0 =
- iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationObjects.mteHotOID.0 = laErrorFlag.1
- iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationObjects.mteHotValue.0 = 1
- iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
SNMP Trap: Backup

A trap is generated on every backup.

Identification

- The originating IP/hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID


Variable Bindings - successful backup

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = "backup completed"
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 0
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Variable Bindings - failed backup

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = "backup failed"
- .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 5
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
**SNMP Trap: Health Emails**

A trap is generated if health email send fail to be generated.

**Identification**

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  
  - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

**Trap OID**

```
dismanEvent-MIBNotifications.mteTriggerFired
```

**Variable Bindings**

- `.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)`
- `snmpTrapOID = mteTriggerFired`
disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: Trouble sending health email'`
disman-EventMIBNotificationObjects.mteHotValue.0 = 1`
- `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`

**SNMP Trap: Disk Latency**

A trap is generated when the disk appears to be slow.

**Identification**

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  
  - `.iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone`
SNMP Trap: Mailbox Status

A trap is generated when the local mailbox reaches 200 plus emails.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  
```plaintext
  .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
```

Variable Bindings - Mailbox email messages reach 200

```plaintext
  .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
  snmpTrapOID = mteTriggerFired
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'WARNING: The total messages in
  the local mailbox for %s has reached in excess of 200'
  disman-EventMIBNotificationObjects.mteHotValue.0 = 1
```
SNMP Trap: Cluster Status

A trap is generated when one or more nodes are down in a cluster.

Identification

• The originating IP / hostname is used to identify the system generating the traps
• The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
• The trap OID is generic for various SNMP events monitored by the system
• The SNMP system name is included as part of the variable binding to assist identification:
  • .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

.iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationObjects.mteTriggerFired

Variable Bindings - One or more nodes are down in the cluster

• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
• snmpTrapOID = mteTriggerFired
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationObjects.mteTriggerFired.0 = 'ERROR: One or more nodes are down in the cluster'
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationObjects.mteHotValue.0 = 1
• .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
SNMP Trap: Database Failover Status

A trap is generated when one or more nodes are down in a cluster.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the Cisco Unified Communications Domain Manager 10.6(1) system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

dismanEvent-MIBNotifications.mteTriggerFired Variable Bindings - db constantly fails over
  - .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
  - snmpTrapOID = mteTriggerFired
disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: The db is failing over constantly within 5 min'
disman-EventMIBNotificationObjects.mteHotValue.0 = 1
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Large Log Files

A trap is generated when large log files are detected in /var/log/.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
SNMP Trap: Network Status

A trap is generated when a network failures occur.

Identification

• The originating IP / hostname is used to identify the system generating the traps
• The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
• The trap OID is generic for various SNMP events monitored by the system
• The SNMP system name is included as part of the variable binding to assist identification:
  * .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID


Variable Bindings - Network failures

• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
• snmpTrapOID = mteTriggerFired
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: Network Failures'
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1
SNMP Trap: Security Updates

A trap is generated when security updates are available.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID

disman-EventMIBNotifications.mteTriggerFired

Variable Bindings - Security updates available.

- .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
- snmpTrapOID = mteTriggerFired
disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'WARNING: Security Updates available'
disman-EventMIBNotificationObjects.mteHotValue.0 = 1
- .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: Memory Usage

A trap is generated for high memory usage.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:
SNMP Trap: NTP Status

A trap is generated if NTP is not configured.

Identification

- The originating IP / hostname is used to identify the system generating the traps
- The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
- The trap OID is generic for various SNMP events monitored by the system
- The SNMP system name is included as part of the variable binding to assist identification:

```
• .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
```

Trap OID

```
dismanEvent-MIBNotifications.mteTriggerFired
```

Variable Bindings - High memory usage

```
• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
• snmpTrapOID = mteTriggerFired
disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: High memory usage'
disman-EventMIBNotificationObjects.mteHotValue.0 = 1
• .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
```

Variable Bindings - Extremely high CPU usage

```
• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
• snmpTrapOID = mteTriggerFired
disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: Extremely high CPU usage'
disman-EventMIBNotificationObjects.mteHotValue.0 = 1
• .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
```
SNMP Trap: DNS status

A trap is generated if DNS is not configured.

Identification

• The originating IP / hostname is used to identify the system generating the traps
• The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
• The trap OID is generic for various SNMP events monitored by the system
• The SNMP system name is included as part of the variable binding to assist identification:
  • .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: DNS status

  dismanEvent-MIBNotifications.mteTriggerFired

Variable Bindings - DNS not configured

• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
• snmpTrapOID = mteTriggerFired
  disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'ERROR: No dns configured for
  <server info>'
  disman-EventMIBNotificationObjects.mteHotValue.0 = 1
• .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone
SNMP Trap: Domain Status

A trap is generated if the domain is not configured.

Identification

• The originating IP / hostname is used to identify the system generating the traps
• The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
• The trap OID is generic for various SNMP events monitored by the system
• The SNMP system name is included as part of the variable binding to assist identification:
  • .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID


Variable Bindings - Domain not configured

• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
• snmpTrapOID = mteTriggerFired
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotTrigger.0 = 'WARNING: No domain configured for <server info>'
• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.disman-EventMIBNotificationObjects.mteHotValue.0 = 1
• .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

SNMP Trap: NTP Offset

A trap is generated when the NTP offset exceeds 1 second.

Identification

• The originating IP / hostname is used to identify the system generating the traps
• The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
• The trap OID is generic for various SNMP events monitored by the system
SNMP Trap: Process Memory Threshold Status

A trap is generated when the process memory exceeds its current threshold.

Identification

• The originating IP / hostname is used to identify the system generating the traps
• The NMS is responsible for associating traps with each managed system, along with clearing of alarms and escalation to the relevant system operator
• The trap OID is generic for various SNMP events monitored by the system
• The SNMP system name is included as part of the variable binding to assist identification:
  - .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

Trap OID


Variable Bindings - Process exceeds memory threshold

• snmpTrapOID = mteTriggerFired
  - .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationsObjects.mteTriggerFired.0 = "<process name: mem_<name> exceeded maximum value of current_threshold with current_reading>"

• .iso.org.dod.internet.mgmt.mib-2.dismanEventMIB.dismanEventMIBNotificationPrefix.dismanEventMIBNotificationsObjects.mteHotValue.0 = 1

• .iso.org.dod.internet.mgmt.mib-2.system.sysName.0 = standalone

• .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = 2 minutes (12065)
MIB List

Cisco Unified Communications Domain Manager 10.6(1) uses standard MIBs that are usually deployed as part of a Network Management System (NMS).

Contact support for a download of the complete archive of MIBs used.

The default net-SNMP packages that ship with Cisco Unified Communications Domain Manager 10.6(1) include:

- ACCOUNTING-CONTROL-MIB
- ADSL-LINE-EXT-MIB
- ADSL-LINE-MIB
- ADSL-TC-MIB
- ADSL2-LINE-MIB
- ADSL2-LINE-TC-MIB
- AGENTX-MIB
- AGGREGATE-MIB
- ALARM-MIB
- APM-MIB
- APPC-MIB
- APPLETALK-MIB
- APPLICATION-MIB
- APPN-DLUR-MIB
- APPN-MIB
- APPN-TRAP-MIB
• APS-MIB
• ARC-MIB
• ATM-ACCOUNTING-INFORMATION-MIB
• ATM-MIB
• ATM-TC-MIB
• ATM2-MIB
• BGP4-MIB
• BRIDGE-MIB
• CAPWAP-BASE-MIB
• CAPWAP-DOT11-MIB
• CHARACTER-MIB
• CIRCUIT-IF-MIB
• CLNS-MIB
• COPS-CLIENT-MIB
• DECNET-PHIV-MIB
• DIAL-CONTROL-MIB
• DIFFSERV-CONFIG-MIB
• DIFFSERV-DSCP-TC
• DIFFSERV-MIB
• DIRECTORY-SERVER-MIB
• DISMAN-EVENT-MIB
• DISMAN-EXPRESSION-MIB
• DISMAN-NSLOOKUP-MIB
• DISMAN-PING-MIB
• DISMAN-SCHEDULE-MIB
• DISMAN-SCRIPT-MIB
• DISMAN-TRACEROUTE-MIB
• DLSW-MIB
• DNS-RESOLVER-MIB
• DNS-SERVER-MIB
• DOCS-BPI-MIB
• DOCS-CABLE-DEVICE-MIB
• DOCS-IETF-BPI2-MIB
• DOCS-IETF-CABLE-DEVICE-NOTIFICATION-MIB
• DOCS-IETF-QOS-MIB
• DOCS-IETF-SUBMGT-MIB
• DOCS-IF-MIB
• DOT12-IF-MIB
• DOT12-RPTR-MIB
• DOT3-EPON-MIB
• DOT3-OAM-MIB
• DPI20-MIB
• DS0-MIB
• DS0BUNDLE-MIB
• DS1-MIB
• DS3-MIB
• DSA-MIB
• DSMON-MIB
• DVB-RCS-MIB
• EBN-MIB
• EFM-CU-MIB
• ENTITY-MIB
• ENTITY-SENSOR-MIB
• ENTITY-STATE-MIB
• ENTITY-STATE-TC-MIB
• ETHER-CHIPSET-MIB
• EtherLike-MIB
• FC-MGMT-MIB
• FCIP-MGMT-MIB
• FDDI-SMT73-MIB
• FIBRE-CHANNEL-FE-MIB
• FLOW-METER-MIB
• FORCES-MIB
• FR-ATM-PVC-SERVICE-IWF-MIB
• FR-MFR-MIB
• FRAME-RELAY-DTE-MIB
• FRNETSERV-MIB
• FRSLD-MIB
• Finisher-MIB
• GMPLS-LABEL-STD-MIB
• GMPLS-LSR-STD-MIB
• GMPLS-TC-STD-MIB
• GMPLS-TE-STD-MIB
• GSMP-MIB
• HC-ALARM-MIB
• HC-PerfHist-TC-MIB
• HC-RMON-MIB
• HCNUM-TC
• HDSL2-SHDSL-LINE-MIB
• HOST-RESOURCES-MIB
• HOST-RESOURCES-TYPES
• HPR-IP-MIB
• HPR-MIB
• IBM-6611-APPN-MIB
• IF-CAP-STACK-MIB
• IF-INVERTED-STACK-MIB
• IF-MIB
• IFCP-MGMT-MIB
• IGMP-STD-MIB
• INET-ADDRESS-MIB
• INTEGRATED-SERVICES-GUARANTEED-MIB
• INTEGRATED-SERVICES-MIB
• INTERFACETOPN-MIB
• IP-FORWARD-MIB
• IP-MIB
• IPATM-IPMC-MIB
• IPFIX-MIB
• IPMCAST-MIB
• IPMROUTE-STD-MIB
• IPOA-MIB
• IPS-AUTH-MIB
• IPSEC-SPD-MIB
• IPV6-FLOW-LABEL-MIB
• IPV6-ICMP-MIB
• IPV6-MIB
• IPV6-MLD-MIB
• IPV6-TC
• IPV6-TCP-MIB
• IPV6-UDP-MIB
• ISCSI-MIB
• ISDN-MIB
• ISIS-MIB
• ISNS-MIB
• ITU-ALARM-MIB
• ITU-ALARM-TC-MIB
• Job-Monitoring-MIB
• L2TP-MIB
• LANGTAG-TC-MIB
• LM-SENSORS-MIB
• LMP-MIB
• MALLOC-MIB
• MAU-MIB
• MGMD-STD-MIB
• MIDCOM-MIB
• MIOX25-MIB
• MIP-MIB
• MOBILEIPV6-MIB
• MPLS-FTN-STD-MIB
• MPLS-L3VPN-STD-MIB
• MPLS-LC-ATM-STD-MIB
• MPLS-LC-FR-STD-MIB
• MPLS-LDP-ATM-STD-MIB
• MPLS-LDP-FRAME-RELAY-STD-MIB
• MPLS-LDP-GENERIC-STD-MIB
• MPLS-LDP-STD-MIB
• MPLS-LSR-STD-MIB
• MPLS-TC-STD-MIB
• MPLS-TE-STD-MIB
• MSDP-MIB
• MTA-MIB
• Modem-MIB
• NAT-MIB
• NEMO-MIB
• NET-SNMP-AGENT-MIB
• NET-SNMP-EXAMPLES-MIB
• NET-SNMP-EXTEND-MIB
• NET-SNMP-MIB
• NET-SNMP-MONITOR-MIB
• NET-SNMP-PASS-MIB
• NET-SNMP-SYSTEM-MIB
• NET-SNMP-TC
• NET-SNMP-VACM-MIB
• NETWORK-SERVICES-MIB
• NHRP-MIB
• NOTIFICATION-LOG-MIB
• OPT-IF-MIB
• OSPF-MIB
• OSPF-TRAP-MIB
• OSPFV3-MIB
• P-BRIDGE-MIB
• PARALLEL-MIB
• PIM-BSR-MIB
• PIM-MIB
• PIM-STD-MIB
• PINT-MIB
• PKTC-IETF-EVENT-MIB
• PKTC-IETF-MTA-MIB
• PKTC-IETF-SIG-MIB
• POLICY-BASED-MANAGEMENT-MIB
• POWER-ETHERNET-MIB
• PPP-BRIDGE-NCP-MIB
• PPP-IP-NCP-MIB
• PPP-LCP-MIB
• PPP-SEC-MIB
• PTOPO-MIB
• PW-ATM-MIB
• PW-ENET-STD-MIB
• PW-MPLS-STD-MIB
• PW-STD-MIB
• PW-TC-STD-MIB
• PW-TDM-MIB
• PerfHist-TC-MIB
• Printer-MIB
• Q-BRIDGE-MIB
• RADIUS-ACC-CLIENT-MIB
• RADIUS-ACC-SERVER-MIB
• RADIUS-AUTH-CLIENT-MIB
• RADIUS-AUTH-SERVER-MIB
• RADIUS-DYNAUTH-CLIENT-MIB
• RADIUS-DYNAUTH-SERVER-MIB
• RAQMON-MIB
• RAQMON-RDS-MIB
• RDBMS-MIB
• RFC1155-SMI
• RFC1213-MIB
• RFC1381-MIB
• RFC1382-MIB
• RFC1414-MIB
• RIPv2-MIB
• RMON-MIB
• RMON2-MIB
• ROHC-MIB
• ROHC-RTP-MIB
• ROHC-UNCOMPRESSED-MIB
• RS-232-MIB
• RSERPOOL-MIB
• RSTP-MIB
• RSVP-MIB
• RTP-MIB
• SCSI-MIB
• SCTP-MIB
• SFLOW-MIB
• SIP-COMMON-MIB
• SIP-MIB
• SIP-SERVER-MIB
• SIP-TC-MIB
• SIP-UA-MIB
• SLAPM-MIB
• SMON-MIB
• SMUX-MIB
• SNA-NAU-MIB
• SNA-SDL-MIB
• SNMP-COMMUNITY-MIB
• SNMP-FRAMEWORK-MIB
• SNMP-IEEE802-TM-MIB
• SNMP-MPD-MIB
• SNMP-NOTIFICATION-MIB
• SNMP-PROXY-MIB
• SNMP-REPEATER-MIB
• SNMP-SSH-TM-MIB
• SNMP-TARGET-MIB
• SNMP-TSM-MIB
• SNMP-USER-BASED-SM-MIB
• SNMP-USM-AES-MIB
• SNMP-USM-DH-OBJECTS-MIB
• SNMP-VIEW-BASED-ACM-MIB
• SNMPv2-CONF
• SNMPv2-M2M-MIB
• SNMPv2-MIB
• SNMPv2-PARTY-MIB
• SNMPv2-PDU
• SNMPv2-TC
• SNMPv2-TM
• SNMPv2-USEC-MIB
• SONET-MIB
• SOURCE-ROUTING-MIB
• SSPM-MIB
• SYSAPPL-MIB
• SYSLOG-MSG-MIB
• SYSLOG-TC-MIB
• T11-FC-FABRIC-ADDR-MGR-MIB
• T11-FC-FABRIC-CONFIG-SERVER-MIB
• T11-FC-FABRIC-LOCK-MIB
• T11-FC-FSPF-MIB
• T11-FC-NAME-SERVER-MIB
• T11-FC-ROUTE-MIB
• T11-FC-RSCN-MIB
• T11-FC-SP-AUTHENTICATION-MIB
• T11-FC-SP-POLICY-MIB
• T11-FC-SP-SA-MIB
• T11-FC-SP-TC-MIB
• T11-FC-SP-ZONING-MIB
• T11-FC-VIRTUAL-FABRIC-MIB
• T11-FC-ZONE-SERVER-MIB
• T11-TC-MIB
• TCP-ESTATS-MIB
• TCP-MIB
• TCPIP-MIB
• TE-LINK-STD-MIB
• TE-MIB
• TIME-AGGREGATE-MIB
• TN3270E-MIB
• TN3270E-RT-MIB
• TOKEN-RING-RMON-MIB
• TOKENRING-MIB
• TOKENRING-STATION-SR-MIB
• TPM-MIB
• TRANSPORT-ADDRESS-MIB
• TRIP-MIB
• TRIP-TC-MIB
• TUNNEL-MIB
• UCD-DEMO-MIB.inc
• UCD-DEMO-MIB
• UCD-DISKIO-MIB.inc
• UCD-DISKIO-MIB
• UCD-DLMOD-MIB.inc
• UCD-DLMOD-MIB
• UCD-IPFILTER-MIB.inc
• UCD-IPFILTER-MIB
• UCD-IPFWACC-MIB.inc
• UCD-IPFWACC-MIB
• UCD-SNMP-MIB-OLD
• UCD-SNMP-MIB.inc
• UCD-SNMP-MIB
• UDP-MIB
• UDPLITE-MIB
• UPS-MIB
• URI-TC-MIB
• VDSL-LINE-EXT-MCM-MIB
• VDSL-LINE-EXT-SCM-MIB
• VDSL-LINE-MIB
• VDSL2-LINE-MIB
• VDSL2-LINE-TC-MIB
• VPN-TC-STD-MIB
• VRRP-MIB
• WWW-MIB
• IANA-ADDRESS-FAMILY-NUMBERS-MIB
• IANA-CHARSET-MIB
• IANA-FINISHER-MIB
• IANA-GMPLS-TC-MIB
• IANA-IPPM-METRICS-REGISTRY-MIB
• IANA-ITU-ALARM-TC-MIB
• IANA-LANGUAGE-MIB
• IANA-MALLOC-MIB
• IANA-MAU-MIB
• IANA-PRINTER-MIB
• IANA-PWE3-MIB
• IANA-RTPROTO-MIB
• IANATn3270eTC-MIB
• IANAifType-MIB
• IPFIX-SELECTOR-MIB

For further information on how to add a MIB, see: http://www.net-snmp.org/wiki/index.php/TUT:Using_and_loading_MIBS.