**Trademark Information**

Polycom® and the names and marks associated with Polycom’s products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners.

Java is a registered trademark of Oracle and/or its affiliates.

**Patent Information**

The accompanying product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

**End User License Agreement**

Use of this software constitutes acceptance of the terms and conditions of the Polycom Resource Manager system end-user license agreement (EULA).

The EULA is included in the release notes document for your version, which is available on the Polycom Support page for the Polycom Resource Manager system.

© 2012 Polycom, Inc. All rights reserved.

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.
## Contents

### 1 Polycom® RealPresence® Resource Manager Overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealPresence Resource Manager System Features and Capabilities</td>
<td>1</td>
</tr>
<tr>
<td>Polycom RealPresence Resource Manager System</td>
<td>2</td>
</tr>
<tr>
<td>Minimum System Requirements</td>
<td>3</td>
</tr>
<tr>
<td>Working in the RealPresence Resource Manager System</td>
<td>3</td>
</tr>
<tr>
<td>- Log Into the RealPresence Resource Manager System</td>
<td>3</td>
</tr>
<tr>
<td>- Field Input Requirements</td>
<td>4</td>
</tr>
<tr>
<td>- Filter and Search a List</td>
<td>4</td>
</tr>
<tr>
<td>- Managing Bandwidth</td>
<td>5</td>
</tr>
<tr>
<td>- Change a Password</td>
<td>7</td>
</tr>
<tr>
<td>- Log Out of the Polycom RealPresence Resource Manager System</td>
<td>7</td>
</tr>
<tr>
<td>- Restart or Shut Down a Polycom RealPresence Resource Manager System</td>
<td>7</td>
</tr>
<tr>
<td>- Emergency Shutdown of a Polycom RealPresence Resource Manager System</td>
<td>8</td>
</tr>
</tbody>
</table>

### 2 System Configuration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add DNS SRV Record for RealPresence Resource Manager System Services</td>
<td>9</td>
</tr>
<tr>
<td>Configure the Connection to an External Enterprise Directory</td>
<td>10</td>
</tr>
<tr>
<td>Configure Redundancy</td>
<td>11</td>
</tr>
<tr>
<td>Set Up Site Topology</td>
<td>11</td>
</tr>
<tr>
<td>Integrate with a Polycom DMA System</td>
<td>11</td>
</tr>
<tr>
<td>Set Up Automatic Provisioning</td>
<td>11</td>
</tr>
<tr>
<td>Set Up Automatic Software Update</td>
<td>12</td>
</tr>
<tr>
<td>Set Up Conference Templates</td>
<td>12</td>
</tr>
<tr>
<td>Set Up Directory Services</td>
<td>13</td>
</tr>
<tr>
<td>Set Up a Certificate for the RealPresence Resource Manager System</td>
<td>14</td>
</tr>
<tr>
<td>Distribute Polycom Applications</td>
<td>14</td>
</tr>
<tr>
<td>- Distribute Polycom CMA Desktop for Windows Systems</td>
<td>14</td>
</tr>
<tr>
<td>- Distribute Polycom CMA Desktop for MAC OS Systems</td>
<td>15</td>
</tr>
</tbody>
</table>

### 3 System Conference Scheduling Overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information for Scheduling Participants and Endpoints</td>
<td>17</td>
</tr>
<tr>
<td>Scheduler Roles</td>
<td>18</td>
</tr>
</tbody>
</table>
Conference Types ................................................. 19
  Future and Anytime Conferences ......................... 19
  Direct and Pooled Conferences ............................. 20
    Direct Conference ........................................ 20
    Pooled Conference ....................................... 21
Scheduler Overview ............................................ 21
Conference Menu Overview .................................... 22
  Conference Menu and Views ................................ 23
  Conference Views—Future and Ongoing ................... 24
  Conference Views—Anytime ................................ 25
Conference States .............................................. 26
Context-Sensitive Conference Actions ..................... 26
User Menu Overview ............................................ 27
  User Menu and Guest Book ................................ 27
  Context-Sensitive Guest Book Actions .................... 28
  Add a Guest to the System Guest Book .................... 28
  Edit a Guest in the System Guest Book .................. 31
  Delete a Guest from the System Guest Book ............... 31

4 Conference Scheduling Operations ....................... 33
  Schedule a Conference ..................................... 33
    Scheduling Future Conferences .......................... 33
    Scheduling Anytime Conferences ........................ 35
  Adding Conference Participants and Guests ............... 36
    Add Conference Participants from a Directory ......... 36
    Add Conference Participants from a Guest Book ....... 37
    Add New Guest Participants ............................. 37
  Copy an Existing Conference .............................. 41
  Edit a Conference .......................................... 41
    Edit a Participant’s Settings ............................ 43
  Writing Conference Notes During a Conference .......... 43
  View Scheduling Information for a Conference .......... 44

5 Advanced Scheduling Operations ......................... 47
  Edit Conference Settings .................................. 47
  Select a Bridge for a Conference ......................... 52

6 Conference and Participant Management Operations ...... 53
  Manage an Active Conference .............................. 53
  Add Additional Participants to an Active Conference .... 56
<table>
<thead>
<tr>
<th>7 Conference and Participant Details</th>
<th>65</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Image</td>
<td>65</td>
</tr>
<tr>
<td>Conference Details</td>
<td>65</td>
</tr>
<tr>
<td>Conference Features</td>
<td>68</td>
</tr>
<tr>
<td>Bridge (MCU) Features</td>
<td>70</td>
</tr>
<tr>
<td>Participants</td>
<td>70</td>
</tr>
<tr>
<td>Participant Details</td>
<td>71</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8 Understanding Endpoint Management</th>
<th>73</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Provisioning</td>
<td>73</td>
</tr>
<tr>
<td>Endpoint Associations and Presence</td>
<td>74</td>
</tr>
<tr>
<td>Endpoint Software Updates</td>
<td>74</td>
</tr>
<tr>
<td>Endpoint Passwords</td>
<td>75</td>
</tr>
<tr>
<td>Standard versus Dynamic Management</td>
<td>75</td>
</tr>
<tr>
<td>Standard Management of Endpoints (Polycom and Third-Party)</td>
<td>75</td>
</tr>
<tr>
<td>Dynamic Management of Endpoints (Polycom Only)</td>
<td>76</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9 Managing Endpoints</th>
<th>79</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Menu, Views, and Lists</td>
<td>79</td>
</tr>
<tr>
<td>Monitor View</td>
<td>80</td>
</tr>
<tr>
<td>Endpoint List in the Monitor View</td>
<td>80</td>
</tr>
<tr>
<td>Actions in the Monitor View</td>
<td>82</td>
</tr>
<tr>
<td>Peripherals View</td>
<td>83</td>
</tr>
<tr>
<td>Peripherals List in the Peripherals View</td>
<td>84</td>
</tr>
<tr>
<td>Actions in the Peripheral View</td>
<td>85</td>
</tr>
<tr>
<td>Manage Endpoints and Peripherals</td>
<td>85</td>
</tr>
<tr>
<td>View Device Details</td>
<td>86</td>
</tr>
<tr>
<td>Add an Endpoint or Find an Endpoint on the Network</td>
<td>90</td>
</tr>
<tr>
<td>Edit an Endpoint</td>
<td>95</td>
</tr>
<tr>
<td>Delete an Endpoint</td>
<td>95</td>
</tr>
</tbody>
</table>
10 Updating Endpoint and Peripheral Software .......................... 101

Software Update Considerations for Multi-Tenancy .......................... 102
Create Software Updates for Endpoints .................................. 102
  List the Serial Numbers for the Endpoints to be Updated ............ 103
  Download the Required Software Package ............................. 104
  Request Update Activation Keys ..................................... 105
  Upload the Software Update ......................................... 106
Using Automatic Software Updates ......................................... 106
  Set an Automatic Software Update Policy ............................ 107
  Automatic Software Update View ................................... 108
    Endpoint List in the Automatic Software Update View ............. 109
  View Automatic Software Update Information for an Endpoint ... 110
  View Automatic Software Update Packages .......................... 112
  Set Maintenance Window for Automatic Software Updates ......... 113
Trial an Automatic Software Update Package ............................... 113
  Create a Local Trial Group .......................................... 114
  Upload the Software Package and Create a Trial Software Update Package .................................................. 114
  Promote the Trial Software Update Package to Production ......... 115
  Delete the Trial Software Update Package .......................... 116
Automatic Software Updates for Peripherals ................................. 116
  View Software Updates for Polycom Touch Controls ................. 117
  Upload Peripheral Software Updates to the RealPresence Resource Manager System ........................................... 118
  Configure Peripheral Updates for Production ....................... 118
  Configure Peripheral Updates for Trial ............................ 120
Using Scheduled Software Updates ......................................... 121
  Supported Endpoints for Scheduled Software Updates .............. 122
Contents

11 Provisioning Endpoints ......................... 127
   Provisioning Best Practices .................. 127
   Provisioning Profile Order and Priority .... 128
   Order of Provisioning Operations .......... 128
   Provisioning in a Multi-Tenancy Environment 128

12 Automatic Provisioning of Endpoints .............. 131
   Automatic Provisioning ....................... 131
   Default Automatic Provisioning Profiles .... 132
   Using Automatic Provisioning ............... 132
   Automatic Provisioning View ............... 133
      Endpoint List in the Automatic Provisioning View 133
      Actions in the Automatic Provisioning View 134
   View the Automatic Provisioning List and Details 134
   Add an Automatic Provisioning Profile .... 134
   Edit an Automatic Provisioning Profile ...... 135
   Edit the Profile Order for an Automatic Provisioning Profile 136
   Clone an Automatic Provisioning Profile .... 136
   Delete an Automatic Provisioning Profile .... 137

13 Bundled Provisioning of Endpoints ................ 139
   How Bundled Provisioning Works ............. 140
   View the Provisioning Bundle List .......... 140
   Download a Provisioning Bundle ............ 141
   Delete a Provisioning Bundle ............... 141
   Bundled Provisioning View ............... 142
      Endpoint List in the Bundled Provisioning View 142
      Actions in the Bundled Provisioning View 142

14 Scheduled Provisioning of Endpoints .............. 143
   How Scheduled Provisioning Works ........... 143
   Scheduled Provisioning Profiles ............ 144
Scheduled Provisioning Notes ........................................ 144
Using Scheduled Provisioning ................................. 145
   View the Scheduled Provisioning List and Details ........ 145
   Add a Scheduled Provisioning Profile ....................... 146
   Edit a Scheduled Provisioning Profile ..................... 146
   Clone a Scheduled Provisioning Profile ................... 147
   Delete a Scheduled Provisioning Profile ................... 147
   Schedule an Endpoint for Provisioning ................. 148
   Check the Status of a Scheduled Provisioning ........ 148
   Clear the Status of Scheduled Provisioning ............ 149
   Cancel a Scheduled Provisioning .......................... 149
   Scheduled Provisioning View .............................. 149
      Endpoint List in the Scheduled Provisioning View .... 149
      Actions in the Scheduled Provisioning View ......... 150

15    Automatic Provisioning Endpoints for SIP Server Integration . . . . . . 153

   SIP Provisioning Considerations .......................... 153
   SIP Server Authentication Requirements ................ 154
   Provision Endpoints with SIP Server Settings ............ 154
      Creating Authentication Information for SIP Endpoints 155
      Import SIP URI Data .................................. 155
      Edit SIP URI Data .................................... 156
      Provision SIP Settings for SIP Server Integration .... 156
      Provision Group for Microsoft Lync or Microsoft Office Communications Server Integration .......... 158
      Microsoft Directory Considerations ................... 159

16    Supported Endpoint Types ................................. 161

   Endpoint Types ........................................... 161
   Considerations for Third-Party Endpoints .............. 164
      Considerations for TANDBERG Endpoints ............... 165
         Enable TANDBERG Endpoints Global Address Book Access 165
         Scheduled Provisioning of Selected TANDBERG Endpoints ... 165
      Considerations for LifeSize Endpoints ............... 184
         Enabling Management of a LifeSize Endpoints ........ 184
         Provisioning of LifeSize Passwords .................. 184
         Scheduled Provisioning of LifeSize Endpoints ........ 185
   Reporting .................................................. 191
   Monitoring ................................................. 191
17 Reference for Provisionable Endpoint Fields .......................... 193
   Endpoint Fields for Automatic Provisioning ...................... 193
   Endpoint Fields for Scheduled Provisioning ..................... 196

18 Endpoint Device Details ........................................... 213
   Endpoint Device Summary Information .......................... 213
   Device Status Information ....................................... 216
   Call Information .................................................. 218
   Device Alerts Information ....................................... 219
   Provisioning Details ............................................. 219
   Software Update Details ......................................... 220

19 Understanding Network Device Management ....................... 223
   Overview of Network Devices .................................. 223
   Monitoring Network Devices .................................... 224
      Monitor View .................................................. 225
      Actions in the Monitor View ................................ 226

20 Managing MCU Bridges ............................................. 229
   MCU View ......................................................... 229
   View Device Details ............................................. 229
   Add an MCU Manually ........................................... 233
   Edit an MCU Bridge ............................................. 235
   Delete an MCU Bridge .......................................... 238
   View Bridge Hardware .......................................... 238
   View Bridge Services ........................................... 239
   View Bridge Conferences ....................................... 239
   View Bridge Ports ............................................... 240
   View Bridge Meeting Rooms .................................... 240
   View Bridge Entry Queues ...................................... 241
   View Bridge Gateway Conferences ............................... 241

21 MCU Device Details ................................................ 243
   MCU H.320 Services ............................................. 243
   MCU H.323 & SIP Services ...................................... 244
   MCU Resources—Polycom RMX Platform ......................... 245
   MCU Device Summary Information .............................. 246
22 Managing a DMA System ..................................... 249
Using a Polycom DMA System with RealPresence Resource Manager System ............................................. 249
  SIP Endpoint Management ........................................ 250
  MCU Management ................................................... 250
  Conference Types Supported By the DMA System .......... 251
  DMA Conference Templates ....................................... 251
  Multi-Tenancy Considerations ................................... 251
  Considerations for Site Topology ................................ 251
  Scheduling Capacity ............................................... 252
Integrating with a Polycom DMA System ......................... 252
  DMA View ............................................................ 252
  Add a Polycom DMA System ...................................... 253
  Edit a Polycom DMA System ..................................... 254
  Delete a Polycom DMA System ................................... 254
Managing DMA Pool Orders ........................................ 254
  View Details of a DMA System Pool Order ................. 255
  Associate a Polycom DMA System Pool Order with an Area ...... 256

23 Managing Border Controllers and Firewalls ............. 257
Manage Polycom VBP Devices ..................................... 257
  VBP View ............................................................ 258
  Add a Polycom VBP Device ...................................... 258
Copy the RealPresence Resource Manager System Certificate to a Polycom VBP Device ..................................... 259
  Edit a Polycom VBP Device ..................................... 259
  Delete a Polycom VBP Device ................................... 259
  Identify Endpoints Using the Polycom VBP Device ...... 260
Manage SBC Devices .................................................. 260
  Add a SBC Device ................................................. 261
  Edit a SBC Device ............................................... 261
  Delete an SBC Device ............................................. 261
  Identify Endpoints Using the SBC Device ................ 262

24 Understanding Users, Groups, and Roles ................. 263
Working with Users .................................................. 263
  Local Users ......................................................... 264
  Enterprise Users .................................................. 264
  Assign Roles to Enterprise Users ............................ 265
Working with Groups .................................................. 265
Local Groups ......................................................... 265
Enterprise Groups .................................................. 265
  Prepare to Use Active Directory ......................... 266
Working with Management Roles and Permissions ........... 266
Understanding User Roles .......................................... 267
Default System Roles and Permissions ....................... 268
  Scheduler Roles, Responsibilities, and Menus .......... 271
  Operator Role, Responsibilities, and Menus ............ 272
  Device Administrator Role, Responsibilities, and Menus . 272
  Auditor Role, Responsibilities, and Menus ............ 273
  Administrator Role, Responsibilities, and Menus ...... 274
Customized Roles and Responsibilities ...................... 274

25 Managing Users .................................................. 277
Manage Users ...................................................... 277
  Search for a User ............................................. 278
  View User Information ....................................... 278
  Add a Local User ............................................. 279
  Edit a User .................................................... 281
  View Role Information for a User ......................... 282
  Delete a User ................................................... 283
  Unlock a User Account ....................................... 283
Import Users ....................................................... 284
  Create a CSV File Containing the User Information you need . 284
  Examples ....................................................... 285
  Import the CSV File .......................................... 286
  Review the Import Details File ................................ 286
Updating Users by Import ......................................... 287
Manage Groups ..................................................... 289
  Add a Local Group ............................................ 289
  Import Enterprise Groups .................................... 290
  Edit a Group .................................................... 291
  Delete a Group .................................................. 291
Manage User Roles .................................................. 291
  Assign Users Roles and Endpoints ......................... 292
  View the List of User Roles .................................. 292
  Add a User Role ................................................ 293
  Edit Permissions for a User Role ......................... 294
  Delete a User Role ............................................ 294
  View the Groups and Users Associated with a User Role . 294
  Assign Users to Manage an Area(s) ....................... 295
Manage System Guest Book ........................................ 296
Guest Book Considerations for Multi-Tenancy .................. 296
User Menu and Guest Book ....................................... 296
Context-Sensitive Guest Book Actions ............................ 297
Add a Guest to the System Guest Book ......................... 297
Edit a Guest in the System Guest Book ......................... 300
Delete a Guest from the System Guest Book .................... 300
Manage Favorites .................................................. 301
Add a Favorites List ............................................... 301
Edit a Favorites List ............................................... 302
Delete a Favorites List ............................................ 302

26 System Reports ................................................. 303
Report Considerations for Multi-Tenancy ....................... 303
Site Statistics Report ............................................. 303
Site Link Statistics Report ....................................... 305
Call Detail Record Report Administration ...................... 306
   Modify the CDR Retention Period .......................... 306
   Schedule Archives of the CDR Report ....................... 306
Endpoint Usage Report ........................................... 307
Conference Usage Report ........................................ 313
Conference Type Report ......................................... 313
View and Export System Log Files ............................. 316
   Change the System Log Level ............................... 317
Download Log Files .............................................. 317
View and Download Audit Log Files ............................ 317
Resource Manager System Report ............................... 318

27 Understanding System Administration ...................... 321
System Dashboard .................................................. 321
   Dashboard Buttons .......................................... 322
   Dashboard Panes ............................................. 322
System Administration Menu .................................... 330

28 Understanding Conference Templates and Settings ....... 333
Direct Conferences vs. Pooled Conferences .................... 333
Direct Conference Templates .................................... 334
   Direct Conference Template Considerations for Multi-Tenancy .. 344
   Direct Conference Template Best Practices .................. 344
DMA (Pooled) Conference Templates ............................ 345
## Contents

DMA System Conference Templates for Multi-Tenancy : 345
Establish Naming Conventions for DMA System Templates : 345
Anytime Conference Templates : 346
Considerations for Anytime Conference Templates : 346
Configure Auto-Terminate : 346
Initiate Conference Dial-out : 347
Conference Settings : 347

### 29 Setting Up Conference Templates and Settings : 349

View the Direct Conference Templates List : 349
Add a Direct Conference Template : 350
Edit a Direct Conference Template : 350
Delete a Direct Conference Template : 351
Set Conference Settings : 351
Disable Conference Auto-Launch : 351
Disable Conference Time Warning : 351
Overbooking Dial-in Participants : 352
Add Customized Text to E-mail Notifications : 352
Edit Customized Text in E-mail Notifications : 353
Delete Customized Text in E-mail Notifications : 353

### 30 Managing Meeting Rooms : 355

Local and Enterprise Meeting Rooms : 355
View the Rooms List : 356
Add a Local Room : 356
Add an Enterprise Room : 358
Edit a Room : 359
Delete a Room : 359

### 31 Understanding Directories : 361

Directory Management Overview : 361
Directory Management Supported Configurations : 362
  Multiple Forests : 362
  Multiple Domains : 362
  Viable options: : 362
Groups : 362
Users : 363
How Global Catalog Searches Work : 364
Accounts Required for the System : 365
  RealPresence Resource Manager System Service Account : 365
Copy an Address Book ................................................. 395

34 Configuring Multi-Tenancy ................................. 397
  Planning For Multi-Tenancy .................................. 397
  Working within a Multi-Tenancy Environment ................. 398
    User Roles within a Multi-Tenancy Environment .............. 398
    System Roles ............................................. 399
    Area Roles ............................................. 399
  Area Conference Participants ............................... 400
  Area Address Books ....................................... 401
  Area User Groups ......................................... 401
  Area Users, Rooms and Associated Endpoints ................. 402
  Area Conference Guests .................................... 402
  Using the Common Pool in a Multi-Tenancy Environment ....... 402
  Area Conference Templates .................................. 402
  Configure Areas ............................................. 403
  Enable Areas ............................................... 404
  Create Areas for Tenants .................................... 404
  Set up Area Management ..................................... 404
    Manage the Area with System Roles ......................... 405
    Manage the Area with Area Roles ........................... 405
  Assign Resources to an Area ................................ 405
    Can Belong to One or No Area .............................. 405
    Can Belong to One or More Areas (or no Area) ............ 406
  Add Users to An Area ....................................... 406
  Configure Site Topology ..................................... 406

35 Managing Areas ............................................. 409
  View All Areas ............................................... 409
  View Information for a Specific Area ....................... 410
  Removing an Area ............................................ 410
    Moving the Contents of an Area .............................. 411
    Deleting an Area and its Resources ......................... 411
    Disabling the Areas Feature ................................ 412
  Customize the Area Logos (system and CMA Desktop) for the Area ... 412

36 Setting Up the RealPresence Resource Manager Server ... 415
  Edit the System Network Settings ............................. 415
  Edit the System Time Settings ................................ 416
Polycom RealPresence Resource Manager System Operations Guide

Integrate with Microsoft Exchange Server for Calendaring Management . . 417
  Associate Sites with Microsoft Exchange Servers ...................... 418
  Assign Calendaring Settings to Provisioning Profiles ................. 419
  Provision the Exchange Mailbox for Calendaring Service-enabled Endpoints ........................................... 419
View Current System Licensing ............................................. 420
System Licensing .............................................................. 420
Add System Licenses .......................................................... 423
  Request a Software License File ........................................ 423
  Update the License File .................................................. 423
Reclaim Polycom CMA Desktop and RealPresence Mobile Licenses .... 424
Add or Remove a System Logo ............................................. 424
Add or Remove a Polycom CMA Desktop Custom Logo ................. 425
Edit the System E-mail Account .......................................... 426

37 Polycom RealPresence Resource Manager System SNMP . 427
  SNMP Overview ............................................................. 427
  Working with SNMP ........................................................ 429
    Enable SNMP Messaging .............................................. 429
    Edit the SNMP Settings for a RealPresence Resource Manager System 429
    Add an SNMP Notification Receiver ................................ 431
  Download RealPresence Resource Manager System MIB Package . 433
  Change the SNMP Communication Port ................................ 435

38 Managing the Database ................................................... 437
  Overview of the RealPresence Resource Manager System Database ... 437
  Database Restoration ...................................................... 437
  Reformat the Existing Database ........................................ 438

39 System Redundancy ......................................................... 439
  System Redundancy Overview ........................................... 439
    Redundant Configuration System Administration ..................... 441
      Licensing ..................................................................... 441
      Data Loss .................................................................... 441
    Considerations for Redundancy ........................................ 441
  Implement a Redundant System .......................................... 442
    Perform a System Backup .............................................. 442
    Perform Network Configuration on Both Servers ................... 442
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect the Servers to Each other Via Cable</td>
<td>443</td>
</tr>
<tr>
<td>Ensure You Have Appropriate Licenses for Both Servers</td>
<td>443</td>
</tr>
<tr>
<td>Configure the Both Servers for Redundancy</td>
<td>443</td>
</tr>
<tr>
<td>License a Redundant System</td>
<td>443</td>
</tr>
<tr>
<td>Failover to a Redundant Server</td>
<td>444</td>
</tr>
<tr>
<td>Discontinue Redundancy</td>
<td>444</td>
</tr>
<tr>
<td>40 Securing the System</td>
<td>447</td>
</tr>
<tr>
<td>Update the System Software</td>
<td>447</td>
</tr>
<tr>
<td>Manage Certificates</td>
<td>448</td>
</tr>
<tr>
<td>Certificates Accepted by the RealPresence Resource Manager System</td>
<td>448</td>
</tr>
<tr>
<td>Certificate Operations</td>
<td>450</td>
</tr>
<tr>
<td>View Certificates and Certificate Details</td>
<td>450</td>
</tr>
<tr>
<td>Create a Certificate Signing Request</td>
<td>452</td>
</tr>
<tr>
<td>Install a Certificate</td>
<td>454</td>
</tr>
<tr>
<td>Upload a Certificate Revocation List</td>
<td>455</td>
</tr>
<tr>
<td>Delete a Certificate</td>
<td>455</td>
</tr>
<tr>
<td>View the Expiration Dates for Certificates and CRLs</td>
<td>456</td>
</tr>
<tr>
<td>Change the System User Interface Timeout and Number of Sessions</td>
<td>456</td>
</tr>
<tr>
<td>Give Enterprise Users Default Scheduler Role</td>
<td>457</td>
</tr>
<tr>
<td>Change the Message for Enterprise Users without a Role</td>
<td>457</td>
</tr>
<tr>
<td>Control Remote Connections to the System</td>
<td>458</td>
</tr>
<tr>
<td>Automatic Registration Synchronization</td>
<td>459</td>
</tr>
<tr>
<td>Set Common Passwords for Endpoints</td>
<td>460</td>
</tr>
<tr>
<td>Disable Common Password for Endpoints</td>
<td>460</td>
</tr>
<tr>
<td>Set Local Account Lockout and Timeout</td>
<td>461</td>
</tr>
<tr>
<td>Set Local Password Requirements</td>
<td>461</td>
</tr>
<tr>
<td>Add Machine Accounts</td>
<td>462</td>
</tr>
<tr>
<td>Change Database Passwords</td>
<td>464</td>
</tr>
<tr>
<td>41 Setting Up Site Topology</td>
<td>467</td>
</tr>
<tr>
<td>Site Topology Set Up</td>
<td>467</td>
</tr>
<tr>
<td>Sites List</td>
<td>469</td>
</tr>
<tr>
<td>Add/Edit Site Dialog Box</td>
<td>470</td>
</tr>
<tr>
<td>Site Links</td>
<td>475</td>
</tr>
<tr>
<td>Add/Edit Site Link Dialog Box</td>
<td>475</td>
</tr>
<tr>
<td>Site-to-Site Exclusions</td>
<td>475</td>
</tr>
<tr>
<td>Territories</td>
<td>476</td>
</tr>
<tr>
<td>Add/Edit Territory Dialog Box</td>
<td>476</td>
</tr>
<tr>
<td>Network Clouds</td>
<td>477</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Add/Edit Network Cloud Dialog Box</td>
<td>477</td>
</tr>
<tr>
<td>Managing Sites</td>
<td>477</td>
</tr>
<tr>
<td>View the Graphical Site Topology</td>
<td>478</td>
</tr>
<tr>
<td>View the Sites List</td>
<td>478</td>
</tr>
<tr>
<td>Add a Site</td>
<td>479</td>
</tr>
<tr>
<td>View Site Information</td>
<td>488</td>
</tr>
<tr>
<td>Assign Locations to a Site</td>
<td>488</td>
</tr>
<tr>
<td>Edit Site Settings</td>
<td>490</td>
</tr>
<tr>
<td>Edit Site Provisioning Settings</td>
<td>490</td>
</tr>
<tr>
<td>Delete a Site</td>
<td>491</td>
</tr>
<tr>
<td>Site Link Operations</td>
<td>491</td>
</tr>
<tr>
<td>View the Site Links List</td>
<td>493</td>
</tr>
<tr>
<td>Add a Site Link</td>
<td>493</td>
</tr>
<tr>
<td>Edit a Site Link</td>
<td>493</td>
</tr>
<tr>
<td>Delete a Site Link</td>
<td>494</td>
</tr>
<tr>
<td>Site-to-Site Exclusions</td>
<td>494</td>
</tr>
<tr>
<td>View the Site-to-Site Exclusion List</td>
<td>494</td>
</tr>
<tr>
<td>Add a Site-to-Site Exclusion</td>
<td>495</td>
</tr>
<tr>
<td>Edit a Site-to-Site Exclusion has</td>
<td>495</td>
</tr>
<tr>
<td>Delete a Site-to-Site Exclusion</td>
<td>495</td>
</tr>
<tr>
<td>Territories</td>
<td>496</td>
</tr>
<tr>
<td>View the Territory List</td>
<td>496</td>
</tr>
<tr>
<td>Add a Territory</td>
<td>496</td>
</tr>
<tr>
<td>Edit a Territory</td>
<td>496</td>
</tr>
<tr>
<td>Delete a Territory</td>
<td>497</td>
</tr>
<tr>
<td>Network Clouds</td>
<td>497</td>
</tr>
<tr>
<td>Multi-tenancy Considerations for Network Clouds</td>
<td>497</td>
</tr>
<tr>
<td>View the List of Network Clouds</td>
<td>497</td>
</tr>
<tr>
<td>Add a Network Cloud</td>
<td>497</td>
</tr>
<tr>
<td>Edit a Network Cloud</td>
<td>498</td>
</tr>
<tr>
<td>Delete a Network Cloud</td>
<td>498</td>
</tr>
</tbody>
</table>

**42 Setting Up Remote Alerts** ....................................... **501**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Up Remote Alerts</td>
<td>501</td>
</tr>
<tr>
<td>Set Up RealPresence Resource Manager System-generated E-mail Account</td>
<td>503</td>
</tr>
<tr>
<td>Enable RealPresence Resource Manager System Remote Alerts</td>
<td>503</td>
</tr>
<tr>
<td>Set RealPresence Resource Manager System Remote Alert Level Settings</td>
<td>504</td>
</tr>
<tr>
<td>Set Endpoint Alert Level Settings</td>
<td>505</td>
</tr>
</tbody>
</table>
Add a Remote Alert Profile ........................................... 507
Associate a Remote Alert Profile With a User ................. 509
Edit a Remote Alert Profile ........................................ 509
Disable a Remote Alert Profile ................................... 510
Delete a Remote Alert Profile ..................................... 510
Disable Remote Alerts ................................................ 510

43  System Management and Maintenance .................. 511
Management and Maintenance Overview ....................... 511
Administrator Responsibilities ................................. 511
Auditor Responsibilities ........................................ 512
Recommended Regular Maintenance ........................... 513

44  System Backup and Recovery Operations ............. 515
Create System Backups ............................................ 515
Backup the System Settings ..................................... 515
Restore the System ................................................ 516
Restore to Factory Default Image ............................... 516
Restore from a Backup Archive ................................ 517

45  System Troubleshooting ................................. 519
Troubleshooting Utilities Dashboard .......................... 519
Troubleshooting Specific Types of Issues ..................... 521
Registration Problems and Solutions ......................... 521
Point-to-Point Calling Problems and Solutions .............. 522
MCU and Gateway Dialing Problems and Solutions ....... 522

A  System Security and Port Usage ....................... 523
Open Inbound Ports on the RealPresence Resource Manager System 523
Outbound Ports Used by the RealPresence Resource Manager System 524

B  MIB Reference ................................................. 527

Index ................................................................. 643
Polycom® RealPresence® Resource Manager Overview

This chapter provides an overview of the Polycom® RealPresence® Resource Manager system and includes these topics:

- “RealPresence Resource Manager System Features and Capabilities” on page 1
- “Polycom RealPresence Resource Manager System” on page 2
- “Minimum System Requirements” on page 3
- “Working in the RealPresence Resource Manager System” on page 3

RealPresence Resource Manager System Features and Capabilities

The RealPresence Resource Manager system is an integrated scheduling and device management platform for video conferencing that can include these features:

- Endpoint management, including provisioning, updating, monitoring, and troubleshooting
- Conference scheduling and monitoring on both RealPresence Resource Manager system resources and the Polycom DMA system (when integrated with the RealPresence Resource Manager system)
- Conference, network device, and system monitoring and management including network typology by geography and visual alarm reporting
- Directory and user management including address books and presence
- The Polycom CMA Desktop client for Windows and MAC operating systems—an easy-to-use video and audio conferencing application that lets your users see and hear the people they call on their desktop system.
• Automatic provisioning for dynamically-managed endpoint systems and scheduled provisioning for standardly-managed and legacy endpoints.

• Automatic software updates for dynamically-managed endpoint systems and scheduled software updates for standardly-managed and legacy endpoints.

• Firewall management capabilities which enable videoconferencing across firewalls.

• Access to user and room directories for on-demand and scheduled calls. Directory services include:
  — Presence and contact list functionality for dynamically-managed endpoints (except for RealPresence Mobile clients).
  — Global Address Book for a single directory structure or Multiple Address Books for multiple managed directories.
  — H.350 and LDAP directory functionality. H.350 defines a directory services architecture for multimedia conferencing for H.323, H.320, SIP and generic protocols.

• Device monitoring and management, including bridges and access controllers such as firewalls and SBCs.

• An optional high-availability, redundant management server configuration.

**Polycom RealPresence Resource Manager System**

The RealPresence Resource Manager system supports up to 10,000 managed devices. It integrates with the DMA 7000 system for call control via H.323 gatekeeper and SIP proxy functions.

The RealPresence Resource Manager system is available in optional High Availability configurations without external database requirements.

The RealPresence Resource Manager system has the following options available (additional charges may apply):

• Integration with a corporate directory

• Integration with Polycom DMA 7000 systems for Virtual Meeting Room (VMR) management and scheduling of virtualized MCU resources

• Multi-tenant management

• Programmatic access through Application Programmers Interfaces (APIs)
Minimum System Requirements

The Polycom RealPresence Resource Manager System Release Notes describe the minimum system requirements for your RealPresence Resource Manager system. To find the most current Release Notes, go to www.support.polycom.com and navigate to the RealPresence Resource Manager system product page.

Working in the RealPresence Resource Manager System

These topics includes some general information you should know when working in the RealPresence Resource Manager system. It includes these topics:

• “Log Into the RealPresence Resource Manager System” on page 3
• “Field Input Requirements” on page 4
• “Filter and Search a List” on page 4
• “Change a Password” on page 7
• “Log Out of the Polycom RealPresence Resource Manager System” on page 7
• “Restart or Shut Down a Polycom RealPresence Resource Manager System” on page 7
• “Emergency Shutdown of a Polycom RealPresence Resource Manager System” on page 8

Log Into the RealPresence Resource Manager System

To log into the RealPresence Resource Manager system web interface, you need:

• Microsoft Internet Explorer® 8.0 or 9.0, Mozilla FireFox® 11 or higher, Apple Safari 10.6 or 10.7, or Google Chrome 17 or higher.
• Adobe® Flash® Player 9.x or 10.x
• The IP address or host name of the RealPresence Resource Manager system server and your username, password, and domain.

The RealPresence Resource Manager system user interface is best viewed with an SXGA display resolution of at least 1280x1024 pixels. The minimum support display resolution is XGA 1024x768 pixels.

Generally, you get three opportunities to enter the correct password. After three failed attempts, the system returns an error message.
To log into a RealPresence Resource Manager system

1. Open a browser window and in the **Address** field enter the RealPresence Resource Manager system IP address or host name.
   - If prompted to install the Adobe Flash Player, click **OK**.
   - If you receive an HTTPS **Security Alert**, click **Yes**.
   - If you see a login banner, click **Accept** to accept the terms and continue.

If you cannot connect to the system, there may be certificate issues.

2. When the RealPresence Resource Manager system **Log In** screen appears, enter your **Username** and **Password**.

3. If necessary, select a different **Language** or **Domain**.

4. Click **Login**.
   
   If you log in as an administrator, you see the RealPresence Resource Manager system **Dashboard**.
   
   For more information about roles and the functionality associated with roles, see “Default System Roles and Permissions” on page 268.

**Field Input Requirements**

While every effort was made to internationalize the RealPresence Resource Manager system, not all system fields accept Unicode entries. If you work in a language other than English, be aware that some RealPresence Resource Manager system fields may accept only ASCII or extended ASCII characters.

**Filter and Search a List**

In the RealPresence Resource Manager system interface, information is often summarized in lists or grids.

Lists that include many items may have filters or searchable fields, which allow you to view a subset of items or search for a specific entry. The available filtering options depend on the type of information in the list. For example in the conference list:

- If you select **Custom Date** as the filter, a calendar filter field appears.
- If you select **Ongoing Plus** as the filter, an attribute option appears. You can select the attribute **Conference Name** and enter all or part of the conference name into the associated text field.

In general, most text filter fields are ASCII only and the RealPresence Resource Manager system search function is a case-insensitive, substring search. That means when you enter a search string, the RealPresence Resource Manager system looks for that string wherever it occurs (beginning, middle, or end) in the word or number.
However, if the RealPresence Resource Manager system is integrated with an Active Directory, the RealPresence Resource Manager system uses the LDAP search function for searches of the directory. LDAP searches are prefix-searches that include an appended wildcard. In this case, when you enter a search string, the system looks for that search string only at the beginning of the indexed fields.

For example, all of the following searches for a participant will find Barbara Smithe:

- Barbara
- Smithe
- Bar
- Smi

To optimize LDAP searches, the RealPresence Resource Manager system (and its dynamically-managed endpoints) searches only indexed LDAP fields and a limited set of attributes. The attributes include:

- ObjectCategory
- memberOf
- DisplayName
- GivenName
- Sn
- Cn
- Samaccountname
- groupType
- distinguishedName
- objectGuid

These are the requested attributes to be returned by the search:

- Sn
- Givenname
- Mail
- Ou
- Objectguid
- Telephonenumber
- Cn
- Samaccountname
- Memberof
- Displayname
- Objectclass
- Title
- localityName
- department

Managing Bandwidth

The Resource Manager system manages the bandwidth between sites and the bandwidth for calls that it schedules within the gatekeeper region it services.
Users with administrator permissions can create bandwidth management policies by setting the following limits. The Resource Manager system applies the lowest value from the settings described here to limit the bit rate of specific calls or conferences.

- **The maximum bit rate for a call at a site.** Set it by editing the site, selecting Routing/Bandwidth, and setting the Call Max Bit Rate.

- **The total bandwidth between sites.** The link type and bandwidth are parameters of the site links between two sites. Set it by editing the site link.

- **The maximum speed (bit rate) for calls across a site link.** This value is also a parameter of the site links between two sites and is set by editing the site link.

- **The specific speed (bit rate) of calls in a conference.** This value is a parameter of the conference, as it is inherited from the conference template. You can achieve granularity of bandwidth management by (a) creating a variety of scheduling roles, (b) creating a variety of conference templates with different conference speeds, (c) associating different scheduling roles with different templates, and (d) associating different users and/or groups with the different scheduling roles.

  For example, you can assign an executive user or group more bandwidth than your typical user. To do this, create a VIP role and assign it scheduling or advanced scheduling permissions. Then create a VIP conference template that has a higher video speed, say 4096 kpbs. Finally, associate the executive user or group with the VIP role.

  There are some things to note in these situations.

  — The Resource Manager system may reduce bandwidth or fail a call if the requested bandwidth is not available.

  — Schedulers with advanced scheduling permissions can choose to change the speed of calls in conference by changing the value for a specific conference. However, the Resource Manager system only allows a connection speed when it is within the parameters set for the site link.

  — Endpoints in a conference may not be capable of transmitting at the requested speed. In this case, they will transmit at the value they can achieve that is closest to the value set for the conference.

- **The maximum speed (bit rate) for receiving calls and the preferred speed for placing calls provisioned on the endpoint.** These values are parameters of the endpoint. For endpoints in dynamic management mode, these values are provisioned as part of the automatic provisioning profile. For endpoints operating in standard management mode, these values are provisioned at the endpoint.

  Note in this case that the endpoint can request a speed when placing a call, but again the Resource Manager system only allows a connection speed when it is within the parameters set for the site topology.
Change a Password

For local users, RealPresence Resource Manager system password requirements (for example, password length and password age) are managed by the RealPresence Resource Manager system administrator. For enterprise users, RealPresence Resource Manager system password requirements are managed by Microsoft Active Directory.

To change your system password

1. Click Settings in the top-right corner of the page.
2. In the Settings dialog box, click Change Password.
3. Enter your Old Password.
4. Enter a New Password.
5. Confirm the new password and click OK.

Log Out of the Polycom RealPresence Resource Manager System

To log out of the RealPresence Resource Manager system

- Click Log Out in the top-right corner of the page.

Restart or Shut Down a Polycom RealPresence Resource Manager System

You have several options for an orderly shutdown or restart of a RealPresence Resource Manager system in non-emergency situations.

The options for an orderly shutdown or restart of the system include:

- Use the Shutdown option on the user interface when you must disconnect the RealPresence Resource Manager system server for some reason; for example, to move it. All RealPresence Resource Manager system functionality is stopped during a Shutdown.
- If the system interface is not available and you must shut down the system, press once (but do not hold) the power switch on the RealPresence Resource Manager system server. This is equivalent to selecting the Shutdown option described previously.
- Use the Restart option on the user interface when you must cycle the RealPresence Resource Manager system for some reason; for example, if the system locks up or loses connection with the database.

If you have access to the RealPresence Resource Manager system user interface, you can also stop future scheduled conferences from starting automatically and wait for active conferences to end before performing an orderly shut down or restart of the system.
During a restart, the system will drop all IP conferences. In general, ISDN conferences will not drop.

**To restart or shut down a RealPresence Resource Manager system**

1. (Optional) To stop future scheduled conferences from starting before you perform the restart or shutdown:
   a. Go to Admin > Conference Settings.
   b. Check the Conference Auto-Launch Disabled check box and click Update.
   c. Go to Admin > Dashboard.
   d. Monitor the Today’s Conferences section to determine when all active conferences are completed.

2. Go to Admin > Dashboard and click Restart or Shutdown, as required.

In a redundant RealPresence Resource Manager system configuration, if you requested a shutdown of the primary server, the system displays a warning indicating that it is initiating a failover.

If you select Restart, it may take the RealPresence Resource Manager system up to 10 minutes to shutdown and then restart all server processes.

**Emergency Shutdown of a Polycom RealPresence Resource Manager System**

You have two options to perform an emergency shutdown of a RealPresence Resource Manager system. Use these options only when you must immediately cut power to the server.

- Press and hold the power switch on the RealPresence Resource Manager system server.
- Pull the system power cord.

After an emergency shutdown (that is when you press and hold the power switch, or you pull the system cord, or you lose power to the system), a system battery may continue to cache information until the battery runs out. In this case, the system enters an error state. To recover, you must connect a keyboard and monitor to the RealPresence Resource Manager system and boot the system to clear the error message. Then the system can begin recovery.
System Configuration

This chapter describes the configuration tasks that may be required, based on your system design and installation, to complete your implementation of a Polycom® RealPresence® Resource Manager system after First Time Setup. It includes these topics:

- “Add DNS SRV Record for RealPresence Resource Manager System Services” on page 9
- “Configure the Connection to an External Enterprise Directory” on page 10
- “Configure Redundancy” on page 11
- “Set Up Site Topology” on page 11
- “Integrate with a Polycom DMA System” on page 11
- “Set Up Automatic Provisioning” on page 11
- “Set Up Automatic Software Update” on page 12
- “Set Up Conference Templates” on page 12
- “Set Up Directory Services” on page 13
- “Set Up a Certificate for the RealPresence Resource Manager System” on page 14
- “Distribute Polycom Applications” on page 14

Add DNS SRV Record for RealPresence Resource Manager System Services

You must configure the DNS server, if you wish it to resolve queries for the RealPresence Resource Manager system by the RealPresence Resource Manager system’s host name or IP address.
We recommend that the DNS server be configured to find the RealPresence Resource Manager system by its fully qualified domain name (FQDN). This ensures that client systems running Polycom CMA Desktop, RealPresence Mobile, and RealPresence m100 can access the RealPresence Resource Manager system.

The DNS should also have entries for your Active Directory server (if different from the DNS).

To dynamically manage endpoints (which includes automatic provisioning, automatic software update, and presence) right out-of-the-box, they must be able to automatically discover the RealPresence Resource Manager system. This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager system. The lookup key for this service record is \_cmaconfig\_tcp. So the record will resemble this:

```
__cmaconfig._tcp.customerdomain.com 86400 IN SRV 0 0 443 Access5.customerdomain.com
```

For more information about DNS, DNS records, and how DNS works, see Microsoft Technet (http://technet.microsoft.com/en-us/library/cc772774(WS.10).aspx).

### Support of Multiple Provisioning Servers

The SRV record must point to the Provisioning Server (RealPresence Resource Manager system) that endpoints will use for auto discovery for Dynamic Provisioning. Two or more provisioning servers may co-reside on a network; however only one may be used for DNS-based discovery of provisioning services.

If more than one provisioning server is used within an environment there is no knowledge or coordination between these environments including, but not limited to:

- No shared directory services
- No shared management or provisioning services
- No shared scheduling
- No shared licenses

### Configure the Connection to an External Enterprise Directory

If during First Time Setup you did not configure your RealPresence Resource Manager system to use an enterprise directory, but need to do so now, see “Understanding Directories” on page 361.

Connecting to an enterprise directory allows users to enter their network usernames and password to log into RealPresence Resource Manager system. It also allows users to access the enterprise directory when selecting conference participants.
Configure Redundancy

You can install the RealPresence Resource Manager system in a fault-tolerant, high-availability, redundant configuration.

A redundant RealPresence Resource Manager system configuration requires the installation of two RealPresence Resource Manager system servers on the same network. During First Time Setup, you are instructed to assign these two servers physical IP addresses. Once the two system servers are installed, see “System Redundancy” on page 439 to finish implementing redundancy.

Set Up Site Topology

The video call routing setup includes site topology and bandwidth management.

You can perform the following tasks:

• Define a site for each physical location in which a LAN or an ISDN connection exists. If you use VPN connections, you can consolidate distinct physical locations into a single logical site to simplify management tasks. You can also define links between sites (site links).

• For each site, define the subnets in which the video endpoint systems are deployed. It is important that the IP addresses used by the endpoints belong to only one subnet at a site.

For more information, see “Setting Up Site Topology” on page 467.

Integrate with a Polycom DMA System

Polycom recommends integrating your RealPresence Resource Manager system with a Polycom DMA system for both call manager (gatekeeper) and conference manager services.

For more information, see “Managing a DMA System” on page 249.

Set Up Automatic Provisioning

The RealPresence Resource Manager system automatic provisioning feature allows an administrator to configure one or more endpoints with the standard set of information the registering endpoints need to operate within the network. This eliminates the need to configure each endpoint individually.
Automatic provisioning is enabled at the endpoint, but the RealPresence Resource Manager system must have automatic provisioning profiles for both the endpoint and the site at which the endpoint resides.

To ensure out-of-box usability, the RealPresence Resource Manager system comes with default automatic provisioning profiles. However, to create your desired user experiences, you should:

- Create customized automatic provisioning profiles for endpoint types.
- Edit the provisioning profile for each site.

For more information, see “Add an Automatic Provisioning Profile” on page 134.

**Set Up Automatic Software Update**

The RealPresence Resource Manager system automatic software update feature allows an administrator to upgrade the software on one or more endpoints with a standard software package. This eliminates the need to upgrade each endpoint individually.

The automatic software update feature is enabled at the endpoint. At start up and at designated intervals, endpoints in automatic software update mode automatically look for a new software update profile and package on the RealPresence Resource Manager system.

To implement automatic software updates, you must create a software update package for each endpoint type you wish to support with updates.

For more information, see “Using Automatic Software Updates” on page 106.

**Set Up Conference Templates**

The RealPresence Resource Manager system uses conference templates and global conference settings to manage system and conference behavior.

The RealPresence Resource Manager system has a Default Template and default global conference settings. You may want to create additional templates with different settings or change the global conference settings.

For more information, see “Understanding Conference Templates and Settings” on page 333.
Set Up Directory Services

Directory services provide information about all users, endpoints, and resources on your video communication network.

To set up RealPresence Resource Manager system directory services, complete the following tasks:

1. Register devices.
   - On endpoints, you can:
     » Set the Global Directory Server (GDS) to point to the RealPresence Resource Manager system IP address or DNS name. We recommend using the IP address to prevent data inconsistencies.
     » Register them to the Polycom DMA system gatekeeper (when it is integrated with your RealPresence Resource Manager system).

Most device information is automatically populated in the RealPresence Resource Manager system through the gatekeeper registration to an integrated DMA system or Global Address Book access. You must review the information for these devices in the RealPresence Resource Manager system Directory Setup page and fill in missing information.

To select endpoints when scheduling conferences, you must first associate them with a user or conference room by editing the specific user or room settings. For more information, see “Understanding Endpoint Management” on page 73.

2. Set up users and associate them with endpoints. Unless your RealPresence Resource Manager system is integrated with an enterprise directory, you must enter all user information manually including endpoint association. If your system is integrated with an enterprise directory, general user information (First Name, Last Name, UserID, Password, E-mail Address) is directly pulled from the directory and cannot be changed. However, you must still associate enterprise users with endpoints. For more information, see “Understanding Users, Groups, and Roles” on page 263.

3. Set up groups, add members, and associate them with provisioning profiles. For more information, see “Understanding Users, Groups, and Roles” on page 263.

4. Set up rooms and associate them with endpoints. Unless your RealPresence Resource Manager system is integrated with an enterprise directory that includes conference rooms, you must enter all room information manually including endpoint association. For more information, see “Managing Meeting Rooms” on page 355.
Set Up a Certificate for the RealPresence Resource Manager System

By default, the RealPresence Resource Manager system uses https and a self-signed certificate for its data interchanges. As a best practice, we recommend replacing the RealPresence Resource Manager system self-signed certificate with a certificate from a Certificate Authority. For more information, see “Manage Certificates” on page 448.

Distribute Polycom Applications

The RealPresence Resource Manager system allows you to download several Polycom applications for use in specific environments. This includes two desktop video applications. These are:

- Distribute Polycom CMA Desktop for Windows Systems
- Distribute Polycom CMA Desktop for MAC OS Systems

These are discussed in the following topics.

Distribute Polycom CMA Desktop for Windows Systems

- On a Windows XP system, the user installing the Polycom CMA Desktop must sign in with administrative privileges. On a Windows Vista system, the user installing the Polycom CMA Desktop must sign into the Administrator account.
- The following procedures assumes you have implemented DNS lookup and Windows authentication for single signon.

To deploy the CMA Desktop client to users, you have at least four distribution options

**Option 1: Distribute the CMA Desktop client via an E-mail link**

You can copy the link for the CMA Desktop client from the CMA system Downloads page into an E-mail that you can send to users.

To do this, copy and paste the CMA Desktop link (for example, http://10.47.9.106/SoftUpdate/vv1/CMADesktop_4_1_1_1010/CMADesktop.exe) from the Downloads page into an E-mail to be sent to users. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the E-mail to users.

**Option 2: Distribute the CMA Desktop client via the management system**

You can provide users access to the RealPresence Resource Manager system, from which they can download the client.
To do this, copy and paste the IP address of the RealPresence Resource Manager system into an E-mail to be sent to users. Include usernames and passwords (as required) in the E-mail to users and instruct them to access the Downloads link.

**Option 3: Distribute the CMA Desktop client via a desktop management or group policy object**

Distribute the .exe installation file as a desktop management or group policy object to a location on client systems and provide directions to users on how to run the executable.

To do this, build a desktop management or group policy object that writes the .exe installation file to a directory (for example, C:\temp) on the user’s local system. Include the command for executing the file in an E-mail to be sent to users. For example:

```
C:\temp\CMA Desktop.exe"/s /v"/qn SBSERVERTYPE=2 SBSERVERADDRESS=nnn.nnn.nnn.nnn
```

Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the E-mail to users.

**Option 4: Distribute the CMA Desktop client via a .zip file**

Zip the .exe installation file and send it in an E-mail to users. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the e-mail to users. For endpoints on the public network that will be accessing the system through a firewall, include the IP address of the firewall system rather than the RealPresence Resource Manager system. The firewall system should then direct traffic to the RealPresence Resource Manager system.

---

**Distribute Polycom CMA Desktop for MAC OS Systems**

- On a MAC system, the user installing the CMA Desktop client must sign in with administrative privileges and an Administrator account.
- The following procedures assumes you have implemented DNS lookup and MAC authentication for single signon

To deploy the CMA Desktop for MAC OS clients to users, you have at least three distribution options:

**Option 1: Distribute the CMA Desktop for MAC OS client via an E-mail link**

You can copy the link for the CMA Desktop for MAC OS clients from the CMA system Downloads page into an E-mail that you can send to users. To do this, copy and paste the CMA Desktop for MAC OS link (e.g., http://10.47.9.136/SoftUpdate/vv1/CMADesktopMac_5_1_0_7458/CMADesktop.dmg) from the Downloads page into an E-mail to be sent to users. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the E-mail to users.
Option 2: Distribute the CMA Desktop Mac client via the management system

You can provide users access to the RealPresence Resource Manager system, from which they can download the client. To do this, copy and paste the IP address of the CMA Desktop Mac system into an E-mail to be sent to users. Include usernames and passwords (as required) in the E-mail to users and instruct them to access the Downloads link.

Option 3: Distribute the CMA Desktop Mac client via a .dmg file

Send the .dmg file in an E-mail to users. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the E-mail to users. For endpoints on the public network that will be accessing the system through a firewall, include the IP address of the firewall system rather than the RealPresence Resource Manager system. The firewall system should then direct traffic to the RealPresence Resource Manager system.
System Conference Scheduling Overview

This chapter provides an introduction to the Polycom® RealPresence Resource Manager® system video conference scheduling functionality and operation. It includes:

- General Information for Scheduling Participants and Endpoints
- Scheduler Roles
- Conference Types
- Scheduler Overview
- Conference Menu Overview
- User Menu Overview

General Information for Scheduling Participants and Endpoints

When you schedule conferences, you select the participants you wish to join the conference from your user directory. Depending on your system configuration, your user directory may be the enterprise directory, the Global Address Book, or one or more local address books. It may also include Guest Book entries.

For participants that have multiple endpoints registered with the RealPresence Resource Manager system, the system selects the participant’s default endpoint. You can change to another endpoint by selecting it from the Call Info list or by editing the participant.

You can schedule participants without endpoints into conferences. You cannot schedule endpoints without owners into conferences. The RealPresence Resource Manager system can be configured to allow you to overbook dial-in participants. In this case, dial-in participants can be scheduled to dial into
multiple conferences during the same time period, but the system reserves resources for the participant for only the first scheduled conference. Dial-out participants cannot be scheduled into multiple conferences at one time.

Also, if you schedule participants into conference as Dial In participants, the conference will require external MCU resources.

**Scheduler Roles**

Using the RealPresence Resource Manager system web scheduling interface, users assigned the default **Scheduler** and **Advanced Scheduler** roles can create one-time or recurring conferences in a manner similar to other calendar applications.

In the **Scheduler** role, you can schedule conferences and view information about your ongoing, past, and future scheduled conferences. You can also add guests to and delete guests from the system **Guest Book**. You cannot view information for conferences that you did not schedule.

Users assigned the **Advanced Scheduler** role can also select bridges and templates and edit some conference settings.

<table>
<thead>
<tr>
<th>Role</th>
<th>Supported Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>View-Only Scheduler</td>
<td>View conferences that other users created</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Add a new conference</td>
</tr>
<tr>
<td></td>
<td>Copy a conference you created</td>
</tr>
<tr>
<td></td>
<td>View details of a conference you created</td>
</tr>
<tr>
<td></td>
<td>Delete a conference you created</td>
</tr>
<tr>
<td>Advanced Scheduler</td>
<td>Add a new conference</td>
</tr>
<tr>
<td></td>
<td>Specify bridges and select templates for new conferences</td>
</tr>
<tr>
<td></td>
<td>Copy a conference you created</td>
</tr>
<tr>
<td></td>
<td>View details of a conference you created</td>
</tr>
<tr>
<td></td>
<td>Edit some conference settings</td>
</tr>
<tr>
<td></td>
<td>Delete a conference you created</td>
</tr>
</tbody>
</table>
Conference Types

This section describes the different types of conferences the system manages. This includes:

- Future and Anytime Conferences
- Direct and Pooled Conferences

**Future and Anytime Conferences**

When you are scheduling conferences using the RealPresence Resource Manager system, you can add two types of conferences:

- **Future** — Conferences that begin immediately or sometime in the future. These conferences have start and end times and can be recurring. Once you have selected a future conference type, next you decide whether you want to create a Direct Conference or a Pooled Conference.
Anytime — Ad hoc conferences that do not have designated start and end times. These conferences are not recurring. To be able to add Anytime conferences, the RealPresence Resource Manager system must be connected to a Polycom DMA system. For more information, see **Scheduling Anytime Conferences**.

**Direct and Pooled Conferences**

When first adding a future conference, you can choose between two types of conferences:

- **Direct Conference**
- **Pooled Conference**

**Direct Conference**

A direct conference is a conference that is managed directly on a RMX system through the RealPresence Resource Manager system.

**Bridge Selection**

When scheduling a Direct conference, users with the **Advanced Scheduler** role can select a bridge to host their conference by selecting the **Single Bridge** option. When they select this option, the system presents a list of bridges that have the capabilities and resources required to host their conference.

Because this bridge list depends on the template selection, users should make their template selection before selecting a bridge. Otherwise, they may select a bridge that cannot meet their conferencing requirements. In this case, the conference will fail to schedule.

Those without the Advanced Scheduler role do not see the bridge selection field at all.

**Bridge Scheduling and Reassignment**

When a conference is scheduled, by default the system automatically assigns the conference to a bridge unless a user with the default **Advanced Scheduler** role intercedes. If that bridge is down at the time the system starts the conference, the RealPresence Resource Manager system attempts to dynamically reassign the conference to another bridge with sufficient capabilities and resources.

- If the system can successfully reassign the conference to another bridge, the conference starts on the newly selected bridge, and the system sends an updated conference E-mail message to all scheduled participants. This updated E-mail includes a new dial-in number that dial-in participants must use to join the conference.
If the system cannot successfully reassign the conference to another bridge, the conference fails to start. The system sends an E-mail to notify the conference organizer of the failure.

Some notes about bridge reassignment:

- The bridge reassignment process only occurs when the system detects that a bridge is down. It does not occur if the system determines that a bridge does not have sufficient resources required to host the conference.
- If the RealPresence Resource Manager system cannot find another bridge with the features and capacity needed to support a conference, the conference fails to start. The system does not attempt to modify the conference settings in any way. Instead, the system sends an E-mail to notify the conference organizer of the failure.

The system will chain bridge reassignments. This means that if the next bridge to which the system assigns a conference is down at the time the system tries to start the conference, the system will try to reassign the conference again.

**Pooled Conference**

A pooled conference is a conference hosted on the Polycom Distributed Media Application™ (DMA) system. Instead of selecting a bridge for your conference, you select a DMA pool order to manage your conference calls.

Pooled conferences are scheduled by the RealPresence Resource Manager system. Resources are allocated at the time of conference initiation by the DMA placing the call on a pool of managed MCUs (RMX or Codian). Using DMA defined priorities, the DMA can manage resource allocation between RealPresence Resource Manager system scheduled conferences and the DMA-initiated ad hoc calls in real-time.

**Scheduler Overview**

As a scheduler, when you log into the RealPresence Resource Manager system, the system displays the main screen with a **Conference** menu. When you click **Conference**, you can select from these conference types: Future, Ongoing, or Anytime.

For more information, see “**Conference Menu and Views**” on page 23.

Anytime conferences are supported if the RealPresence Resource Manager system is connected to a Polycom DMA system.
The User menu allows you to select Guest Book and view users or add guests to the guest directory. For more information, see “User Menu and Guest Book” on page 27.

You might also see these menu items:

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings.</strong> Click here to display a Settings dialog box with the following information:</td>
</tr>
<tr>
<td>• User Name</td>
</tr>
<tr>
<td>• Remote Server</td>
</tr>
<tr>
<td>• Software Version</td>
</tr>
<tr>
<td>• Font Size</td>
</tr>
<tr>
<td>In this dialog box, you can also:</td>
</tr>
<tr>
<td>• Change the font size used in your display of the RealPresence Resource Manager system web interface.</td>
</tr>
<tr>
<td>• Change your password, if you are a local system user.</td>
</tr>
<tr>
<td><strong>Downloads.</strong> Click here to display the Downloads dialog box with the downloadable applications compatible with the RealPresence Resource Manager system. Downloadable applications may include:</td>
</tr>
<tr>
<td>• Polycom CMA Desktop PC or MAC client (including the path to the application)</td>
</tr>
<tr>
<td>• Polycom File Verification Utility</td>
</tr>
<tr>
<td><strong>Log Out.</strong> Click here to log out of the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>The RealPresence Resource Manager system has an inactivity timer. If you are logged into the system but do not use the interface for a specified period of time, the system automatically logs you out.</td>
</tr>
<tr>
<td><strong>Help.</strong> Links to the RealPresence Resource Manager system online help.</td>
</tr>
</tbody>
</table>

**Conference Menu Overview**

This section includes some general information you should know about the Conference menu and views. It includes these topics:

• Conference Menu and Views
• Conference Views—Future and Ongoing
• Conference Views — Anytime
• Context-Sensitive Conference Actions
Conference Menu and Views

The Conference menu provides these views of the Conference list:

- **Future** — Displays the list of future scheduled conferences in the main window. Use this view to view and edit future conferences. After selection, the Future-Only filter is enabled.

- **Ongoing** — Displays the list of active scheduled and Anytime conferences in the main window. Use this view to manage ongoing conferences. After selection, the Ongoing-Plus filter is enabled.

- **Anytime** — Displays the list of anytime conferences in the main window. Use this view to manage anytime conferences. Anytime conferences are ad hoc conferences that require no start and stop times.

Users can only work with the conferences that appear in their Conference list. By default, schedulers see only their conferences in the Conference list. Operators see all the conferences on the system. However, when areas are defined, operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

The Future and Ongoing Conference views have these sections.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Views</td>
<td>The views you can access from the page.</td>
</tr>
<tr>
<td>Conference Actions</td>
<td>The set of available commands. The constant commands in the Conference views are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Refresh</strong> — Use this command to update the system display with current information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> — Use this command to schedule a new video or audio conference.</td>
</tr>
<tr>
<td></td>
<td>For the list of context-sensitive Conference commands, see “Context-Sensitive Conference Actions” on page 26.</td>
</tr>
<tr>
<td>Conference List</td>
<td>The context-sensitive Conference list for the selected view.</td>
</tr>
<tr>
<td>Conference Details</td>
<td>Displays information about the selected conference. For more information, see “Conference Details” on page 65.</td>
</tr>
<tr>
<td>Conference Features</td>
<td>Displays the status of system features for the selected conference. For more information, see “Conference Features” on page 68.</td>
</tr>
<tr>
<td>Participants</td>
<td>Displays the list of participants for the selected conference. For more information, see “Participants” on page 70.</td>
</tr>
<tr>
<td>Participant Details</td>
<td>Displays information about the participant selected in the Participants list. For more information, see “Participant Details” on page 71.</td>
</tr>
</tbody>
</table>
## Conference Views—Future and Ongoing

The Conference list in both the Future and Ongoing views includes these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Use the filter to display other views of the conference list, which include:</td>
</tr>
<tr>
<td></td>
<td>• Future Only - Displays scheduled conferences that have not yet started</td>
</tr>
<tr>
<td></td>
<td>• Today Only - Displays scheduled conferences (completed, active, or future) for the current day.</td>
</tr>
<tr>
<td></td>
<td>• Custom Date - Displays scheduled conferences (completed, active, or future) for a selected day. Select the day from the calendar.</td>
</tr>
<tr>
<td></td>
<td>• Ongoing Plus - Displays active and future scheduled conferences for the day. You can further filter this request by Conference Name, Endpoint Name, Bridge, and Area.</td>
</tr>
<tr>
<td></td>
<td>• Today Plus - Displays scheduled conferences (completed, active, or future) for the current day, and all future conferences. You can further filter this request by Conference Name, Endpoint Name, Bridge, and Area.</td>
</tr>
<tr>
<td></td>
<td>• Yesterday Plus - Displays completed scheduled conferences for yesterday and earlier. You can further filter this request by Conference Name or Area.</td>
</tr>
<tr>
<td></td>
<td>These filters apply to scheduled conferences only. Ad hoc conferences are not displayed in the filtered list.</td>
</tr>
<tr>
<td></td>
<td>For information on filters, see “Filter and Search a List”.</td>
</tr>
<tr>
<td>Export as Excel file</td>
<td>Click this button to download the currently displayed Conference list to a Microsoft Excel spreadsheet.</td>
</tr>
<tr>
<td>Status</td>
<td>The state of the conference. For more information, see “Conference States” on page 26.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of scheduled conference. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Video Conference — All conference participants have video endpoints.</td>
</tr>
<tr>
<td></td>
<td>• Direct Conference — Direct conferences are hosted on resources managed by the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td></td>
<td>• Pooled Conference — Pooled conferences are hosted on resources managed by the Polycom DMA system.</td>
</tr>
<tr>
<td></td>
<td>• Audio Only Conference — All conference participants have audio endpoints. Audio only conferences require an MCU.</td>
</tr>
<tr>
<td></td>
<td>• Recurring Conference — The conference is one in a recurring series.</td>
</tr>
</tbody>
</table>
## Conference Views — Anytime

Anytime conferences are supported if the Resource Manager system is connected to a Polycom DMA system.

The **Conference** list in Anytime view has these fields.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the conference</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the conference</td>
</tr>
<tr>
<td>Virtual Meeting Room (VMR)</td>
<td>Virtual meeting room assigned to the conference</td>
</tr>
<tr>
<td>Owner</td>
<td>Person who is assigned control of the conference</td>
</tr>
<tr>
<td>Created On</td>
<td>Date on the local system when the conference was originally added</td>
</tr>
<tr>
<td># Participants</td>
<td>Number of participants in the conference</td>
</tr>
</tbody>
</table>
Conference States

Conferences may be in the following states.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Future Conference</td>
<td>Scheduled conference that has not yet started. This conference state is possible in all views except the Yesterday Plus view.</td>
</tr>
<tr>
<td>Completed Conference</td>
<td>A scheduled conference that occurred in the past. This conference state is possible in all views except the Future and Ongoing Plus view.</td>
</tr>
<tr>
<td>Active Conference</td>
<td>A conference that is still active/ongoing. This conference state is possible in all views except the Future and Yesterday Plus view.</td>
</tr>
</tbody>
</table>
| Active Alerts       | The bridge on which the active/ongoing conference is being hosted has sent an alert. Examples of events that will trigger a bridge alert are:  
• A participant is connected in secondary mode (audio only).  
• A conference is not yet full (for example, not all scheduled participants have joined the conference).  
  Note  
  This state applies to Direct Conferences only. |
| Conference End Warning| The conference is ending. For example, the conference is in its last five minutes unless someone extends it. |

Context-Sensitive Conference Actions

Besides the constant Refresh and Add actions, the Conference Actions section may include these context-sensitive actions depending on the type of conference selected.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available for future conferences only</td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>Use this command to edit a conference that you have added. For more information, see “Edit a Conference” on page 41.</td>
</tr>
<tr>
<td>Available for future and past conferences</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Use this command to delete a conference that you have added.</td>
</tr>
</tbody>
</table>
User Menu Overview

This section includes some general information you should know about the Conference menu and views. It includes these topics:

- User Menu and Guest Book
- Context-Sensitive Guest Book Actions
- Add a Guest to the System Guest Book
- Edit a Guest in the System Guest Book
- Delete a Guest from the System Guest Book

User Menu and Guest Book

By default, schedulers, operator, and administrators have access to the User Menu and Guest Book.

The Guest Book is a local system directory that includes guest participants who were either:

- Explicitly added to the Guest Book.
- Saved to the Guest Book while being added as conference participants.

They are referred to as static entries because they are not imported through the dynamically updated enterprise directory or included in the system Global Address Book. The Guest Book is limited to 500 entries. The Guest Book has these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The guest's first and last name.</td>
</tr>
</tbody>
</table>
Add a Guest to the System Guest Book

To add a guest to the system Guest Book

1. Go to User > Guest Book and click Add Guest.
2. Configure the Guest Information section of the Add New Guest dialog box.
3 If the guest has an H.323 (IP) endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>The guest’s first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The guest’s last name.</td>
</tr>
<tr>
<td>Email</td>
<td>The guest’s E-mail address. The system only validates the structure of the E-mail address.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the guest’s endpoint system. This is a free-form field that the system does not validate.</td>
</tr>
<tr>
<td>Dial Type</td>
<td>Specify the protocol that the guest’s endpoint supports: H.323 (IP), SIP (IP), or H.320 (ISDN). This selection will determine what other sections of the Add New Guest dialog box you will need to complete.</td>
</tr>
<tr>
<td>Join Mode</td>
<td>Specify whether the guest’s endpoint is an audio or video endpoint.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>A guest may have multiple endpoints. Create a separate Guest Book entry for each endpoint.</td>
</tr>
<tr>
<td>Dial Options</td>
<td>Specify whether the guest will dial into conferences, or require that the system dial out to the guest.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>To support both options, create a separate Guest Book entry for each.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Type and Number</td>
<td>The format and value of the number that the MCU must resolve to contact the guest. This may be an IP address, E.164 address, H.323, or Annex-O.</td>
</tr>
<tr>
<td>Extension</td>
<td>The specific dial string for the guest. For Annex-O dialing, enter the H.323.alias@IP here, for example:</td>
</tr>
<tr>
<td></td>
<td>• 1001@11.12.13.14</td>
</tr>
<tr>
<td></td>
<td>• <a href="mailto:1001@domain.com">1001@domain.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
<tr>
<td></td>
<td>• username@11.12.13.14</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Polycom endpoints must register with a gatekeeper before they’ll attempt an Annex-O call.</td>
</tr>
</tbody>
</table>
If the guest has a SIP (IP) endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sip URI</td>
<td>The SPI URI the MCU must resolve to contact the guest.</td>
</tr>
<tr>
<td>MCU Service</td>
<td>Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at <em>Any Available Service</em> unless you have specific knowledge of MCU services.</td>
</tr>
</tbody>
</table>

If the guest has an H.320 (ISDN) endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Modified Dial Number</td>
<td>Select this option first (as needed) as it will determine the other fields you must configure.</td>
</tr>
<tr>
<td>Country</td>
<td>(Not available when <em>Use Modified Dial Number</em> is selected.) The country to which the system will dial out to the guest. Click <em>Select</em> to view a list of country codes.</td>
</tr>
<tr>
<td>Area/City Code</td>
<td>(Not available when <em>Use Modified Dial Number</em> is selected.) The area code to which the system will dial out to the guest.</td>
</tr>
<tr>
<td>Number</td>
<td>The participant’s phone number.</td>
</tr>
<tr>
<td>Extension</td>
<td>Cannot be configured.</td>
</tr>
<tr>
<td>MCU Service</td>
<td>Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system has registered. Leave this at <em>Any Available Service</em> unless you have specific knowledge of MCU services.</td>
</tr>
</tbody>
</table>

Click **OK**.
Edit a Guest in the System Guest Book

To edit a guest in the system Guest Book
1. Go to User > Guest Book and select the guest of interest.
2. Click Edit Guest.
3. Change the Guest Information section and endpoint information sections of the Add New Guest dialog box, as needed. For more information about these fields, see “Add a Guest to the System Guest Book” on page 28.
4. Click OK.

Delete a Guest from the System Guest Book

To delete a guest from the system Guest Book
1. Go to User > Guest Book and select the guest of interest.
2. Click Delete Guest.
3. Click Yes to confirm the deletion.
Conference Scheduling Operations

This chapter describes the Polycom® RealPresence Resource Manager® system conference scheduling operations. It includes these topics:

- Schedule a Conference
  - Scheduling Future Conferences
  - Scheduling Anytime Conferences
  - Adding Conference Participants and Guests
  - Copy an Existing Conference
- Edit a Conference
- Edit a Participant’s Settings
- Writing Conference Notes During a Conference
- View Scheduling Information for a Conference

Schedule a Conference

By default, only Schedulers and Operators can schedule conferences.

Scheduling Future Conferences

Users with the following default user roles are allowed to schedule Future conferences: scheduler, operator, area operator and area scheduler.

To schedule a new Future conference

1. Go to Conference > Future and under Conference Actions, click Add.
2. On the conference scheduling page, select either Direct Conference or Pooled Conference.
**Direct Conference** - A conference hosted on RealPresence Resource Manager system. For more information, see “Direct Conference” on page 20.

**Pooled Conference** - A conference hosted on the Polycom Distributed Media Application™ (DMA) system. For more information, see “Pooled Conference” on page 21.

3. Enter a new **Conference Name** or accept the default name.

4. Set a conference **Start Date, Start Time**, and either an **End Time** or **Duration**.

5. To make the conference recurring, click **Recurrence** and in the Appointment Recurrence dialog box, set:
   - Recurrence frequency (Daily, Weekly, or Monthly)
   - Recurrence day (Sunday through Saturday)
   - Recurrence range (Start date and End After occurrences or End by date)

   The maximum number of recurrences is 365.

6. Click **OK**.

7. For Pooled conferences, under **DMA Pool Orders**, accept the default pool order or select one from the list.

   The DMA Pool Order indicates the set of managed MCUs which can be used to fulfill conference resource needs. Select a pool order based upon your geographic and capacity guidelines.

8. If available, select a **Lecturer**, **Video Chairperson**, or **Owner**.

9. For an audio-only conference, change the Conference Type to **Audio Only**.

10. For Direct conferences, under **Bridge Selection**, do one of the following:
    - **Auto Bridge**: Allows the system to select a bridge.
    - **Single Bridge**: Allows you to select an MCU from the **Scheduled MCU** list to host the conference.

11. To change the **Conference Template**, click Default Template or Default Audio Template and select a different template, if available.

12. **Assigned Area** is view-only. It displays the area to which the conference owner belongs. This field is only visible when areas are enabled.
13 **Conference Passcode** is view-only. It displays the passcode originally configured by the administrator for the conference.

14 **Owner Passcode** is view-only. It displays the passcode originally configured by the administrator for the selected conference owner.

15 Once you are satisfied with the conference settings, click **Schedule Conference**.

• Conference templates provide default conference settings. When you select a different template, you are selecting the default conference settings for your conference.

• The **Default Template** and **Default Audio Template** are available to all users who can schedule conferences. Other templates may also be available if they have been assigned to users with your role.

• The **Default Template** and **Default Audio Template** are stored in the system database and their names are not localized.

• Conference templates for Direct Conferences are defined in the RealPresence Resource Manager system, while conference templates for Pooled Conferences are defined in the DMA system.

### Scheduling Anytime Conferences

Users with the following default user roles are allowed to schedule Anytime conferences: Scheduler, Advanced Scheduler, Operator, Area Operator and Area Scheduler.

Unlike Future conferences, Anytime conferences do not have designated start and end times. Once an Anytime conference is configured, conferences can be started at any time by authorized participants. The following events occur when a new Anytime conference is added:

• A participant with scheduling permissions creates a new Anytime conference and the conference is assigned a virtual meeting room (VMR) number.

• The following passcodes are automatically generated:
  
  — **Owner passcode**: Required to launch an Anytime conference.

• All Anytime conference participants receive an E-mail indicating the VMR number. The owner will also receive the owner passcode needed to launch the conference.
• When a participant dials the VMR number and enters the owner passcode, all dial-out participants are automatically called. If a participant dials into the VMR, they are allowed into the conference or placed on hold until someone dials in and enters the owner passcode.

• The conference continues until all participants hang up the call.

To schedule a new Anytime conference
1 Go to Conference > Anytime and under Conference Actions, click Add.
2 Enter a new conference Name or accept the system-generated name.
3 Enter a Description for the conference.
4 At Template, select a template that your administrator has suggested you use for Anytime conferences.
5 Select an Owner for the conference.
6 Under Search for Participants and Rooms, do one of the following to add a participant or a guest:
   a To add a participant: Enter a last and first name and click Add Participants. Scroll through the list and click once to add a participant. When finished, click Close.
   b To add a guest: Enter a last and first name and click Add from Guest Book. Scroll through the list and click once on a name in the list. When finished, click Close.
7 To save the conference details, click Save.

Adding Conference Participants and Guests

You may add participants to conferences in the following ways:
• Add Conference Participants from a Directory
• Add Conference Participants from a Guest Book
• Add New Guest Participants

These tasks are for all conference types: Future, Ongoing, and Anytime.

Add Conference Participants from a Directory

To add conference participants from the local directory or enterprise directory
1 Enter all or part of a participant’s Last Name or First Name into one of the name fields and click Add Participants.

The Add Participants dialog box appears with the list of participant names that meet your search criteria.
Select the participant of interest’s name from the list.

The participant’s name appears in the underlying Selected Participants and Rooms list.

Repeat steps 1 and 2 to add all domain participants and then click Close.

Add Conference Participants from a Guest Book

To add a guest from the Guest Book

1. Click Add from Guest Book.

2. In the Add from Guest Book dialog box, select the guest of interest’s name from the list.

   The guest’s name appears in the underlying Selected Participants and Rooms list.

3. Repeat step 2 to add all participants from the Guest Book and then click Close.

Add New Guest Participants

To add a new guest (participants not available through the local directory, enterprise directory, or Guest Book)

1. Click Add Guest.

2. Configure these fields in the Add Guest dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>The guest's first name.</td>
</tr>
</tbody>
</table>
If the guest has an **H.323 (IP)** endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>The guest’s last name.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The system allows you to add multiple users with the same first and last name into the Guest Book.</td>
</tr>
<tr>
<td>Email</td>
<td>The guest’s E-mail address. The system only validates the structure of the E-mail address.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The E-mail field is ASCII only.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the guest’s endpoint system. This is a free-form field that the system does not validate.</td>
</tr>
<tr>
<td>How will the participant join the conference</td>
<td>Specify how the participant will join the conference.</td>
</tr>
<tr>
<td></td>
<td>• <strong>In Person</strong> — The participant will attend the conference by going to a room that is included in the conference or joining another participant who is attending the conference.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Audio Only</strong> — The participant will attend the conference by telephone. The system will either call out to the participant or the participant will dial in.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use Video</strong> — The participant will attend the conference using a video endpoint system. The system will either call out to the participant or the participant will dial in.</td>
</tr>
<tr>
<td></td>
<td>This selection will in part determine what other fields of the Add Guest dialog box you will need to complete.</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>(Video only) Set as required. You can change the connection speed for an endpoint up to the maximum speed specified by the conference template.</td>
</tr>
<tr>
<td>Dial Options</td>
<td>Specify whether the guest will dial into the conference or require that the system dial out to the guest.</td>
</tr>
<tr>
<td>Dial Type</td>
<td>Specify the protocol that the guest’s endpoint supports: H.323 (IP), SIP (IP), or H.320 (ISDN). This selection determines what other sections of the Add New Guest dialog box you need to complete.</td>
</tr>
</tbody>
</table>

---

If the guest has an **H.323 (IP)** endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension</td>
<td>Use this field to connect the conference to another conference on another MCU. In this field, specify the conference ID or passcode for the conference on the other MCU.</td>
</tr>
</tbody>
</table>
If the guest has a **SIP (IP)** endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU Service</td>
<td>Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at <strong>Any Available Service</strong> unless you have specific knowledge of MCU services.</td>
</tr>
<tr>
<td>SIP URI</td>
<td>The SIP URI that the MCU must resolve to contact the guest.</td>
</tr>
<tr>
<td>MCU Service</td>
<td>Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at <strong>Any Available Service</strong> unless you have specific knowledge of MCU services.</td>
</tr>
<tr>
<td>Encryption</td>
<td>To encrypt the endpoint data, choose Auto, Yes, or No from the list.</td>
</tr>
</tbody>
</table>

If the guest has an **H.320 (ISDN)** endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>The participant’s phone number</td>
</tr>
<tr>
<td>Extension</td>
<td>The participant’s phone extension</td>
</tr>
<tr>
<td>MCU Service</td>
<td>Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system has registered. Leave this at <strong>Any Available Service</strong> unless you have specific knowledge of MCU services.</td>
</tr>
<tr>
<td>Encryption</td>
<td>To encrypt the endpoint data, choose Auto, Yes, or No from the list.</td>
</tr>
</tbody>
</table>

3 Select **Save to Guest Book** to include this guest in the system **Guest Book**.

4 Click **OK**.

The guest’s name appears in the **Selected Participants and Rooms** list.

5 Adjust the conference date and time as needed to match participant and endpoint availability.

a Review their availability and adjust the conference date and time as needed.
To edit a participant’s dial settings, select the participant from the Selected Participants and Rooms list and click Edit. For more information on editing participants settings, see “Edit a Participant’s Settings” on page 43.

6 To add conference rooms to the Selected Participants and Rooms list:
   a Click Select Site.
   b Select the site of interest from the site list
      The conference room list for the selected site appears.
   c Select the conference room of interest from the list.
      The conference room name appears in the underlying Selected Participants and Rooms list.
   d Repeat steps b and c to add all required conference rooms and then click OK.

7 If you have the Advanced Scheduler role, now is the time to assign conference leadership roles, edit conference settings, and make bridge selections. For more information, see “Advanced Scheduling Operations” on page 47.

8 To edit a participant’s dial settings, select the participant from the Selected Participants and Rooms list and click Edit. For more information on editing participants settings, see step 5 on page 43.

9 When finished, click Schedule.
   The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification E-mail appears with a message indicating Conference Successfully Scheduled.

10 To exit without sending an E-mail message to participants, click Skip Email.

11 To send an E-mail notification to participants:
   a Copy additional people on the notification and/or add notes about the conference.
   b As needed, add information in the Enter additional notes to include in the email section.
Copy an Existing Conference

Future and past conferences can be copied as a template for a future conference. Users can only copy conferences that appear in their Conference list. By default, schedulers see only their conferences in the Conference list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To copy a conference

1. Go to the appropriate conference view.
2. Select the conference of interest and click Copy.
3. If you used a template other than the default when you created the conference, reselect the template.
4. Make the required changes to the conference date, participants, rooms, or other settings. For information on performing these tasks, see “Schedule a Conference” on page 33.
5. When finished, click Schedule Conference.
   The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification E-mail appears with a message indicating Conference Successfully Scheduled.
6. To exit without sending an updated E-mail message to your participants, click Skip Email.

Edit a Conference

Future and Anytime conferences can be edited. Users can only edit the conferences that appear in their Conference list. By default, schedulers see only their conferences in the Conference list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.
To edit a Future conference

1. Go to Conference > Future.
2. Select the conference of interest and click Edit.
3. If you select a recurring conference, a dialog box appears asking if you want to edit all conferences in the series or just the selected one. Make the appropriate choice and click Edit.

   The conference scheduling page appears.
4. To change the template, click Default Template or Default Audio Template and select a different template, if available.

   - Conference templates provide default conference settings. When you select a different template, you are selecting the default conference settings for your conference.
   - The Default Template and Default Audio Template are available to all users who can schedule conferences. Other templates may also be available to you if they have been assigned to users with your role.
   - The Default Template and Default Audio Template are stored in the system database and their names are not localized.

5. Make the required changes to the conference date, participants, rooms, or other settings. For information on performing these tasks, see “Schedule a Conference” on page 33.
6. When finished, click Schedule.

   The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification E-mail appears with a message indicating Conference Successfully Scheduled.
7. To exit without sending an updated E-mail message to your participants, click Skip Email.
8. To send an updated E-mail to your participants:
   a. Copy additional people on the notification and/or add notes about the conference.

      Note that the To, CC, and BCC fields are ASCII only.
   b. Click Send.

      The system sends the updated conference notification E-mail message. The Future view appears. Your conference appears in the conference list.
Edit a Participant’s Settings

You can edit conference participant settings after you have added them to a scheduled conference. If the conference is ongoing or already taken place, you can no longer edit the settings.

Users can only work with the conferences that appear in their Conference list. By default, schedulers see only their conferences in the Conference list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default users assigned other roles cannot view conferences.

To edit a participant’s settings

1. Go to Conference > Future.
2. Select the conference of interest and click Edit.
3. If you select a recurring conference, a dialog box appears asking if you want to edit all conferences in the series or just the selected one. Make the appropriate choice and click Edit.
4. In the conference scheduling page, select the participant of interest from the Selected Participants and Rooms list and click Edit.
5. In the Edit Participant Settings dialog box, you can edit the participant settings as required:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints</td>
<td>Select an endpoint from the list.</td>
</tr>
<tr>
<td>Dial Options</td>
<td>Select either Dial-In or Dial-Out.</td>
</tr>
<tr>
<td>Dial Type</td>
<td>Select either H.323 (IP) or SIP (IP).</td>
</tr>
</tbody>
</table>

6. When finished, click OK.

Writing Conference Notes During a Conference

Participants with scheduler permissions can write conference notes during an ongoing conference.

To create a conference note

>> Click the Conference Notes pane, type a note, and click Save.

The note becomes visible on any other browser where other users are attending the same conference.
View Scheduling Information for a Conference

Users can only view scheduling information for the conferences that appear in their Conference list. By default, schedulers see only their conferences in the Conference list, while operators see all the conferences on the system, unless areas are defined. When areas are defined, operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To view the scheduling information for a Future or Ongoing conference

1. To see the scheduling information for a future conference, go to Conference > Future. To see the scheduling information for an active conference, go to Conference > Ongoing.
2. From the Filter list, select the conference type of interest.
3. Select the conference to view from the list. Under Conference Actions, click View.

The View conference page appears displaying the following details about the selected Future or Ongoing conference:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Name</td>
<td>The system- or scheduler-assigned name of the conference. By default, the system assigns a conference name and appends the day and date to that name.</td>
</tr>
<tr>
<td>Start Date</td>
<td>The date on which the conference started or will start.</td>
</tr>
<tr>
<td>End Date</td>
<td>The date on which the conference is scheduled to end.</td>
</tr>
<tr>
<td>Duration</td>
<td>The scheduled duration of the conference in hours and minutes.</td>
</tr>
<tr>
<td>Recurrence</td>
<td>The recurrence information for the conference.</td>
</tr>
<tr>
<td>Owner</td>
<td>The designated person in control of the conference.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of conference, either Audio-Video or Audio only.</td>
</tr>
</tbody>
</table>
To return to the conference list, click Back to List. You might need to scroll down to see the Back to List button.

To view the scheduling information for an Anytime conference

1 To see scheduling information for an Anytime conference, click Conference > Anytime or under Views, click Anytime.

   The list of anytime conferences is displayed.

2 To view details about a particular anytime conference, select the conference, then view the Participants pane or click Edit.

   For descriptions of these details, see Conference Views — Anytime.

3 The following Participant details are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the participant</td>
</tr>
<tr>
<td>Call Info</td>
<td>Call information about the participant, including Video Dial-Out, Video Dial-In, or an IP address</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Call Type</td>
<td>Information about the call type, either H.323, SIP (IP), or H.320 (ISDN).</td>
</tr>
<tr>
<td>Dial Options</td>
<td>The type of participant call, either Dial-In or Dial-Out.</td>
</tr>
</tbody>
</table>
Advanced Scheduling Operations

This chapter describes how users with the Advanced Scheduler role have more options when scheduling conferences using the Polycom® RealPresence Resource Manager™ system.

When scheduling conferences, advanced schedulers can:

- Edit Conference Settings
- Select a Bridge for a Conference

**Edit Conference Settings**

By default, users with the Advanced Scheduler role can overwrite certain conference template settings as described here.

Two conferences scheduled with the same template may have different settings and behavior if they are hosted on different types of MCUs. Minimize or eliminate such differences by ensuring that all MCUs are similarly configured and that all Resource Manager system templates are synchronized with RMX profiles.

Schedulers can edit conference settings only for scheduled conferences. They cannot edit conference settings for active conferences.

**To edit conference settings**

1. On the conference scheduling page, as you are adding or editing a conference, click **Edit Conference Settings**.

2. As needed, configure these settings on the **Conference Settings** dialog box. The settings that you can edit may depend on the template selected.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference ID</td>
<td>By default, the system assigns a Conference ID. You can change this ID to permit integration with third-party scheduling tools. This identifier must be 8 or less numeric digits. Note that the RealPresence Resource Manager system compares the Conference ID to its database to verify that it is unique. If it is not unique, you will be prompted to enter a new Conference ID.</td>
</tr>
<tr>
<td>Conference Passcode</td>
<td>By default, the system assigns an 15-digit Conference Passcode and provides this passcode to participants within the content of the conference notification E-mail. You can change this passcode to another 9- through 16-digit number.</td>
</tr>
<tr>
<td>Enable Chairperson</td>
<td>You can select a video chairperson to control the conference from his or her video endpoint system. The video chairperson must have a video endpoint system and Chairperson conferences require an MCU.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes</strong></td>
</tr>
<tr>
<td></td>
<td>• If the conference template has the Conference Requires Chairperson parameter enabled, then Enable Chairperson is automatically selected and cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>• If a conference is scheduled on a Polycom RMX system and the RMX profile has Conference Requires Chairperson selected but the template does not, and the conference is scheduled without a chairperson, then all users will remain in the waiting room and will not be able to join the conference.</td>
</tr>
<tr>
<td></td>
<td>• Polycom RMX 1000 systems do not support the Chairperson feature.</td>
</tr>
<tr>
<td>Chairperson Passcode</td>
<td>If Enable Chairperson is selected, the system assigns an 15-digit Chairperson Password and provides this password to the video chairperson in a separate E-mail. If Enable Chairperson is selected, the chairperson must enter this 15-digit password at his or her video endpoint to assume control of the conference. You can change this password to another 4- through 16-digit number.</td>
</tr>
</tbody>
</table>
### Dial Options
You have three options:
- To create a conference for which the same dial-in information and a PIN code are assigned to all conference participants, use the **Dial-In** setting. This setting allows participants to dial in from an audio or video endpoint and connect to the same conference on the MCU.
- To dial out to all participants in the conference, use the **Dial-Out** setting.
- To allow participants both options, select **Dial-In+Dial-Out**.

**Note**
When you change a conference from **Dial-In** to **Dial In+Dial Out**, the selected resources remain set to **Dial-In**. You must change them manually.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always Use MCU</td>
<td>Forces the conference to an MCU and prevents video endpoints from connecting to each other directly. This setting is automatically selected and cannot be changed when <strong>Audio Only</strong> is the conference type or when <strong>Enable Chairperson</strong> is selected.</td>
</tr>
<tr>
<td>Video Mode</td>
<td>Determines the initial layout on a video endpoint's monitor for a multipoint conference that requires an MCU. The options are:</td>
</tr>
<tr>
<td></td>
<td>- Switching. Indicates that the display changes each time the speaker changes, and everyone sees the current speaker.</td>
</tr>
<tr>
<td></td>
<td>- Select a <strong>Frame Count</strong>, then select the specific layout for the frames.</td>
</tr>
<tr>
<td></td>
<td>Available layouts are Continuous Presence settings.</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>Specifies the maximum connection speed for endpoints in the conference. Individual endpoints that specify a lower connection speed connect at that lower speed. Endpoints that specify a higher connection speed connect at the speed identified in the conference template.</td>
</tr>
<tr>
<td></td>
<td>If you select a higher speed than an endpoint can support, the system reduces the speed that endpoint; however, the conference uses the default connection speed for endpoints that can match it. If you place the calls through an endpoint with an embedded MCU, the behavior depends on the capabilities of that endpoint.</td>
</tr>
</tbody>
</table>

**Polycom, Inc.**
If the conference is configured for Chairperson or Lecturer modes, assign participants leadership roles:

a. To assign a participant the lecturer role, in the Lecturer field select the participant’s name from the list.

b. To assign a participant the video chairperson role, in the Video Chairperson field select the participant’s name from the list.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit Rate (continued)</td>
<td>When the dial speed is higher than the number of channels defined in the H.320 service for the endpoint, you receive a warning. To continue, lower the dial speed to less than or equal to the ISDN capability of the endpoint. Higher speed is important for high-quality video in a conference. Because higher speeds use greater bandwidth, scheduling a high-bandwidth conference may limit the number of conferences that you can reserve at one time.</td>
</tr>
</tbody>
</table>
| People + Content         | Controls the ability for one endpoint to send two types of data—a data stream and a video stream—over the same bandwidth to display people and content. The receiving endpoint handles the two video streams differently and may display them on separate screens or through video switching mode. Endpoints that do not support the selected method connect with either video through IP or audio only through ISDN. Select from these available settings:  
  • None. Select this option when dual data streams are not required.  
  • People + Content (H.329). This enables the industry standard H.239 dual streams for endpoints that support H.239 or the Polycom proprietary People+Content dual streams for older Polycom endpoints without H.239 capabilities. The MCU requires that conferences with People + Content use a minimum speed of 192 K.  
  • People and Content VO. This Polycom proprietary technology works with PictureTel endpoints. Select this option for older endpoints.  
  • Duo Video. This setting supports IP and ISDN and is available with TANDBERG endpoints, in which one part of the conference is set as the video conference and the other as the presentation conference. |
• If the **Lecturer** or **Video Chairperson** features are not available, the selected template does not support these features.
• To be assigned **Lecturer**, a participant must have a manageable video endpoint.

4 Continue on to “Select a Bridge for a Conference” on page 52, as required, or return to adding or editing the conference, as described in “Conference Scheduling Operations” on page 33.
Select a Bridge for a Conference

By default when scheduling a conference, the RealPresence Resource Manager system will automatically select a bridge for the conference. However, users with the Advanced Scheduler role can select a specific bridge for a conferences.

To select a single bridge for a conference

1. When you’re adding or editing a conference, after you’ve made all of your other conference configuration choices, from the Bridge Selection list select Single Bridge, which causes the Scheduled MCU field to be displayed.

2. From the Scheduled MCU list, select an MCU to host the conference.
Conference and Participant Management Operations

This chapter describes the Polycom® RealPresence Resource Manager® system conference and participant management operations. It includes these topics:

- Manage an Active Conference
- Add Additional Participants to an Active Conference
- Add a Room to an Active Conference
- View the Video of a Participant in an Active Conference
- Join an Active Conference
- Add a Participant from a Favorites List to an Active Conference
- Add/Save a Participant to a Favorites List
- Manage a Participant’s Endpoint During a Conference
- View a Participant’s Details During a Conference
- Terminate an Active Conference
- Delete a Conference

Manage an Active Conference

The Manage Conference page provides a detailed view of a single active conference and allows an operator to make changes to the conference.

To manage an active conference

1. Go to Conference > Ongoing.
2. From the list of All Conferences, select the conference of interest and click Manage.
The conference page appears in a new tab displaying the **Participants** list. The **Participants** list displays these settings:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The state of the participant’s connection as identified by an icon. Hover over the icon to determine the status.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of conference as identified by an icon. Hover over the icon to determine the type.</td>
</tr>
<tr>
<td>Name</td>
<td>The participant’s name.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>The name assigned to the participant’s endpoint when it registered or was added to the system.</td>
</tr>
</tbody>
</table>
| Access  | The endpoint’s network interface type. Possible values include:  
  • H323  
  • ISDN  
  • SIP |
| Address | The IP address, or ISDN number of the participant’s endpoint (if a dial-out), or SIP URI. |
| Bit Rate| The sum of the audio and video data transfer rate (in kbps) of the participant’s endpoint. |
| Dial Mode| How the participant joined the call. Possible values include:  
  • Audio or Video Dial-In  
  • Audio or Video Dial-Out |
| Bridge  | The MCU on which the participants call resides. |

3 Use these conference actions as needed:

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>Schedule a new conference that duplicates the selected conference settings.</td>
</tr>
<tr>
<td>View</td>
<td>View information for the selected conference.</td>
</tr>
<tr>
<td>Terminate</td>
<td>End an active conference.</td>
</tr>
<tr>
<td>Extend Duration</td>
<td>Extend the duration of an active conference.</td>
</tr>
<tr>
<td>Action</td>
<td>Use this action to...</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change Layout</td>
<td>For applicable endpoints. Change the default video layout for the conference display.</td>
</tr>
<tr>
<td></td>
<td>• Switching. Indicates that the display changes each time the speaker changes, and everyone sees the current speaker.</td>
</tr>
<tr>
<td></td>
<td>• Select a <strong>Frame Count</strong>, then select the specific layout for the frames. The available layouts are Continuous Presence settings.</td>
</tr>
<tr>
<td>Add Participant</td>
<td>Add one or more participants to the selected conference.</td>
</tr>
<tr>
<td>Add Guest</td>
<td>Add a guest to the selected conference.</td>
</tr>
<tr>
<td>Add Room</td>
<td>Add one or more rooms to the selected conference.</td>
</tr>
<tr>
<td>Add Favorites</td>
<td>Add participants from one of your Favorites lists to the selected conference.</td>
</tr>
<tr>
<td>Join Conference</td>
<td>Join the conference, monitor the conference, and talk with participants as needed.</td>
</tr>
</tbody>
</table>

Use these participant actions as needed:

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mute or Unmute Audio</td>
<td>Mute or unmute the selected participant's audio line into the conference. This option appears only when the conference is running on an external MCU. The Audio column in the Participants list shows the current status of this setting.</td>
</tr>
<tr>
<td>Block or Unblock Video</td>
<td>Block or unblock the selected participant's video line into the conference. This option appears only when the conference is running on an external MCU. The Video column in the Participants list shows the current status of this setting.</td>
</tr>
<tr>
<td>Connect or Disconnect</td>
<td>Disconnect or reconnect the selected participant to the conference. A disconnected participant is still associated with the conference and cannot be scheduled for other conferences.</td>
</tr>
<tr>
<td>Remove</td>
<td>Remove the selected participant from the Participants list at which time the participant can be scheduled for another conference.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Send a message to the selected participant's registered Polycom endpoint. The message appears briefly on the monitor for the selected video endpoint.</td>
</tr>
</tbody>
</table>
Add Additional Participants to an Active Conference

Operators can add additional participants to an active conference.

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledge Help</td>
<td>Acknowledge a request for help and send a message to the requesting endpoint.</td>
</tr>
<tr>
<td>Manage Device</td>
<td>Open the web-based user interface for the selected participant’s endpoint in a new browser window.</td>
</tr>
<tr>
<td>Save as Favorite</td>
<td>Function available when the selected participant has an associated endpoint to which the system can dial out. Save the selected participant to an existing Favorites List.</td>
</tr>
<tr>
<td>Connect All New</td>
<td>Function available only when the system is displaying the <strong>New Conference Participants</strong> list. Initiates the system dial out to new participants.</td>
</tr>
</tbody>
</table>

**Dial Out** is the only **Dial Option** the system allows for adding participants to an active conferences.

To add additional conference participants to an active conference

1. Go to **Conference > Ongoing**.
2. From the list of **All Conferences**, select the conference of interest and click **Manage**.
3. To add participants from the local directory or enterprise directory:
   a. Click **Add Participant**.
   b. Enter all or part of a participant’s **Last Name** or **First Name** into the appropriate field and click **Search**.
      
      A list appears of participant’s names that meet the search criteria.

- Depending on the search domain, the search function may return different results. See “**Filter and Search a List**” on page 4.
- The search results only include users associated with endpoints.
The search results only include users associated with endpoints.

c  Select the participant’s name from the list.
   The participant’s name appears in the underlying New Conference Participants list.

d  Repeat steps a through c to add all domain participants and then click Close.

e  If necessary, edit the new participants’ settings. See “Edit a Participant’s Settings” on page 43.

4  To add participants from the Guest Book:
   a  Click Add Guest.
   b  From the Guest Book dialog box, select the guest’s name from the list.
      The guest’s name appears in the underlying New Conference Participants list.
   c  Repeat step b to add all guest participants and then click Close.

5  To add new guest participants (participants not available from the local directory, enterprise directory, or Guest Book), see step on page 37.

6  To initiate the system dial out to new participants, select the participants of interest from the New Conference Participants list and click Connect New Participants.
   The system dials out to the participants and adds them to the conference.

Add a Room to an Active Conference

To add a room to an active conference

1  Go to Conference > Ongoing.

2  From the list of All Conferences, select the conference of interest and click Manage.

3  From the Conference Actions list, click Add Room.

4  From the Add Room dialog box, select the site location of the room.
   The list of conference rooms at the site appears.
5 Select the conference room of interest.
   The conference room name appears in the underlying New Conference Participants list.

6 Click Close.

7 To initiate the system dial out to the room, select the room from the New Conference Participants list and click Connect New Participants.
   The system dials out to the room endpoint system and adds the room to the conference.

**View the Video of a Participant in an Active Conference**

**To view the video of a participant in an active conference**

1 Go to Conference > Ongoing.

2 From the list of All Conferences, select the conference of interest and click Manage.

3 Select a participant from the Participants list.
   The selected participant’s video appears in the Conference Image section of the interface.

4 Click Shuffle to shuffle to the next participant’s video.

**Join an Active Conference**

By default, users assigned the Operator role can join an active conference to offer conference support.

**To join an active conference**

1 Go to Conference > Ongoing.

2 From the list of All Conferences, select the conference of interest and click Manage.

3 From the Conference Actions list, click Join Conference.
   The Join Conference dialog box appears.

4 If you have multiple endpoints, choose the endpoint to use to join the conference.
5 Click Join Conference.
Your endpoint is added to conference with your video blocked but your audio not muted.

Add a Participant from a Favorites List to an Active Conference

By default, users assigned the Operator role can work with favorites lists.

To add a participant from a favorites list to an active conference
1 Go to Conference > Ongoing.
2 From the list of All Conferences, select the conference of interest and click Manage.
3 From the Conference Actions list, click Add Favorites.
4 From the Favorites List, expand the list of interest.
   The names of the participants in the list is displayed.
5 Select the participant of interest from the list.
   The participant’s name appears in the underlying New Conference Participants list.
6 Repeat steps 4 and 5 to add all participants from Favorite’s List and then click Close.
7 To initiate the system dial out to new participants, select the participants of interest from the New Conference Participants list and from the New Participants Action menu, click Connect New Participants.
   The system dials out to the participants and adds them to the conference.

Add/Save a Participant to a Favorites List

By default, users assigned the Operator role can work with favorites lists.

To add or save a conference participant to a favorites list
1 Go to Conference > Ongoing.
2 From the list of All Conferences, select the conference of interest and click Manage.
3 From the Participants list, select the participant of interest.
4 From the Participant Actions menu, click Save as Favorite.
The names of the participants in the list is displayed.

5 From the Save as Favorite Participant dialog box, select the Favorite List to which to save the participant and click OK.

Manage a Participant’s Endpoint During a Conference

The Manage page also allows operators to manage conference participant’s endpoints.

To manage a participant’s endpoint
1 Go to Conference > Ongoing.
2 Select the conference of interest and click Manage.
The Participants list appears.
3 To view participants geographically, click .
4 Double-click on the participant of interest.
5 Use these participant actions as needed. These actions are also available from the View Participants Details dialog box.

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mute or Unmute Audio</td>
<td>Mute or unmute the selected participant's audio line into the conference. This option appears only when the conference is running on an external MCU. The Audio column in the Participants list shows the current status of this setting.</td>
</tr>
<tr>
<td>Block or Unblock Video</td>
<td>Block or unblock the selected participant's video line into the conference. This option appears only when the conference is running on an external MCU. The Video column in the Participants list shows the current status of this setting.</td>
</tr>
<tr>
<td>Connect or Disconnect</td>
<td>Disconnect or reconnect the selected participant to the conference. A disconnected participant is still associated with the conference and cannot be scheduled for other conferences.</td>
</tr>
</tbody>
</table>
View a Participant’s Details During a Conference

This procedure describes how to view details for a participant’s endpoint while it is in conference.

To view a participant’s endpoint details
1. Go to Conference > Ongoing.
2. Select the conference of interest and click Manage.
   The Participants list appears.
3. To view participants geographically, click .
4. Double-click on the participant of interest.
   The View Participant Details dialog box appears with the Call Properties displayed. It includes the Near End and Far End video, the Participant’s name, Status, Errors, Warnings, Endpoint Type, Address, Access, and Bit Rate.
   It also includes a list of Participant Actions. For more information about these actions, see “Manage a Participant’s Endpoint During a Conference” on page 60.
To view additional participant details, change the selection in the Call Properties drop-down menu.

- If you select Device, you’ll see these participant details:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Type</td>
<td>Usually the endpoint model, such as Polycom HDX system.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address for the endpoint.</td>
</tr>
<tr>
<td>Site</td>
<td>The location of the endpoint as identified by its IP address and the subnet of the site.</td>
</tr>
<tr>
<td>Gatekeeper</td>
<td>The gatekeeper with which the endpoint is registered.</td>
</tr>
<tr>
<td>Presence</td>
<td>Whether or not the endpoint is registered with a Presence service, so that its availability can be reported.</td>
</tr>
<tr>
<td>Device Managed</td>
<td>Whether or not the endpoint is registered with a Provisioning service, so that it can be configured automatically.</td>
</tr>
<tr>
<td>ISDN Line Status</td>
<td>The status of the ISDN line. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Operational ☑️</td>
</tr>
<tr>
<td></td>
<td>• Non-operations ✗</td>
</tr>
<tr>
<td></td>
<td>This field is blank for the following endpoint types: RMX, GW/MCU, Other, and TANDBERG.</td>
</tr>
<tr>
<td>Alias Type</td>
<td>If the endpoint has an alias designation, the type of alias. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown.</td>
</tr>
<tr>
<td>Alias Value</td>
<td>Value for the alias type shown.</td>
</tr>
</tbody>
</table>

- If you select Call Details, you’ll see these participant details:
If you select Call Quality of Service, you’ll see these standard service measurements: Total Packet Loss, % Packet Loss, Audio Packet Loss, Video Packet Loss, Audio Jitter, and Video Jitter.

### Table: Video and Audio Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Protocol</td>
<td>The video connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• H.261</td>
</tr>
<tr>
<td></td>
<td>H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions.</td>
</tr>
<tr>
<td></td>
<td>• H.263</td>
</tr>
<tr>
<td></td>
<td>H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions.</td>
</tr>
<tr>
<td></td>
<td>• H.264</td>
</tr>
<tr>
<td>Video Format</td>
<td>The video format, both transmission (Tx) and reception (Rx), the endpoint is using.</td>
</tr>
<tr>
<td>Video Rate</td>
<td>The video bandwidth negotiated with the far site.</td>
</tr>
<tr>
<td>Video Rate Used</td>
<td>The actual video bandwidth used in the call to the far site.</td>
</tr>
<tr>
<td>Video Frame Rate</td>
<td>Specifies the frame rate to use.</td>
</tr>
<tr>
<td>Video FEC Errors</td>
<td>The number of Forward Error Correction (FEC) errors that have been corrected in the current call.</td>
</tr>
<tr>
<td>Cause Code</td>
<td></td>
</tr>
<tr>
<td>Audio Rate</td>
<td>The audio bandwidth negotiated with the far site.</td>
</tr>
<tr>
<td>Audio Protocol</td>
<td>The audio connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using.</td>
</tr>
</tbody>
</table>

To terminate an active conference

1. Go to Conference > Ongoing.
2. Select the conference of interest and click Terminate.
3. Click Terminate to confirm the termination.
Delete a Conference

Users can delete future or past conferences. Users cannot delete active conferences.

To delete a conference
1. Go to Conference > Future.
2. To delete a past conference, select the appropriate filter (such as Yesterday Plus).
3. Select the conference of interest and click Delete.
4. If you select a recurring conference, a dialog box appears asking you if you want to delete just the conference you selected or all conferences in the series. Make the appropriate choice. Active conferences in the series cannot be deleted.
5. Click Delete to confirm the deletion.

The conference is deleted. For future conferences, the system E-mails the change to the conference owner and participants and releases the participant and room resources.
This chapter lists the conference and participant detail fields for reference. It includes:

- Conference Details
- Conference Features
- Bridge (MCU) Features
- Participants
- Participant Details

### Conference Image

The Conference Image section displays the selected participant’s video. Click Shuffle to shuffle to the next participant’s video.

### Conference Details

The Conference Details section has these fields.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creator</td>
<td>Name of the person who created the conference. Not applicable for ad hoc conferences.</td>
</tr>
<tr>
<td>Owner</td>
<td>Name of the owner of the conference, if an owner is selected. Note: Not applicable for Anytime conferences.</td>
</tr>
<tr>
<td>Start Date/Time</td>
<td>For a scheduled conference, the start date and time of the conference and the time difference between the local time and the standard time. For an unscheduled conference, the date and time the conference started.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Duration</td>
<td>For a scheduled conference, how long the conference is scheduled to last. For a completed conference, how long the conference actually lasted.</td>
</tr>
<tr>
<td>End Date/Time</td>
<td>The date and time the conference ended</td>
</tr>
</tbody>
</table>
| Type             | The type of conference. Possible values include:  
|                  | • Audio  
|                  | • Audio-Video                                                                                                                                    |
| Status           | The state of the conference. Possible values include:  
|                  | • ActiveAlerts  
|                  | • Declined  
|                  | • Finished  
|                  | • Future                                                                                                                                           |
| Recurring        | Whether or not the conference was scheduled as a recurring conference                                                                                   |
| Connection       | Connection information about the conference. Possible values include:  
|                  | • Multipoint  
|                  | • Point To Point  
|                  | • Gateway  
|                  | • Embedded Multipoint                                                                                                                               |
| Bit Rate         | The rate (in kbps) at which to transfer the conference audio or video data                                                                           |
| Conf Monitoring ID | System-assigned ID used for troubleshooting                                                                                                            |
| Video Session Type | Type of video session: Video Switching or Continuous Presence.                                                                                     |
## Video Layout

The video layout for the conference. Possible values are:

- VIDEO_SWITCHING
- CP_1X1
- CP_1X2
- CP_2X1
- CP_2X2
- CP_3X3
- CP_1AND5
- CP_1AND7
- CP_1X2VER
- CP_1X2HOR
- CP_1AND2HOR
- CP_1AND2VER
- CP_1AND3HOR
- CP_1AND3VER
- CP_1AND4VER
- CP_1AND4HOR
- CP_1AND8CENTRAL
- CP_1AND8UPPER
- CP_1AND2HORUPPER
- CP_1AND3HORUPPER
- CP_1AND4HORUPPER
- CP_1AND8LOWER
- CP_4X4
- CP_2AND8
- CP_1AND12
- CP_1X1QCIF
- CP_1X2FLEX
- CP_1AND2HORRFLEX
- CP_1AND2HORLRFLEX
- CP_1AND2HORUPPPRFLEX
- CP_1AND2HORUPPERLRFLEX
- CP_2X2UPPPRFLEX
- CP_2X2UPPERLRFLEX
- CP_2X2DOWNRFLEX
- CP_2X2DOWNLRFLEX
- CP_2X2RFLEX
- CP_2X2LRFLEX
- CP_UNKNOWN

## Schedule ID

System-assigned ID used for troubleshooting
### Conference Features

The **Conference Features** section has these fields.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Passcode</td>
<td>The conference passcode, which is assigned either by the system or the scheduler.</td>
</tr>
<tr>
<td>Chairperson Option</td>
<td>Indicates whether or not the conference requires a chairperson.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The RMX 1000 system does not support the Chairperson feature.</td>
</tr>
<tr>
<td>Chairperson Passcode</td>
<td>The passcode the chairperson must enter to take control of the conference. Not applicable when no chairperson is designated.</td>
</tr>
<tr>
<td>Chairperson</td>
<td>The name of the chairperson. Not applicable when no chairperson is designated.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lecture Mode</td>
<td>The type of Lecture Mode, if any, that was selected when the conference was created. Possible values are None, Lecture, and Presentation.</td>
</tr>
<tr>
<td>Lecturer</td>
<td>The name of the lecturer. Not applicable when Lecture Mode is None.</td>
</tr>
<tr>
<td>Lecture View Switching</td>
<td>Indicates whether or not automatic switching between participants is enabled.</td>
</tr>
<tr>
<td>Dual Stream Mode</td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• People+Content</td>
</tr>
<tr>
<td></td>
<td>• Visual Concert PC</td>
</tr>
<tr>
<td></td>
<td>• Visual Concert FX</td>
</tr>
<tr>
<td>T120 Rate</td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• HMLP - Var</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 384</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 320</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 256</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 192</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 128</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 6.4</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 62.4</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 14.4</td>
</tr>
<tr>
<td></td>
<td>• MLP - Var</td>
</tr>
<tr>
<td></td>
<td>• MLP - 64.4</td>
</tr>
<tr>
<td>End Time Alert</td>
<td>Whether or not the system alerts participants to the end of the conference by playing an end tone</td>
</tr>
<tr>
<td>Entry Tone</td>
<td>Whether or not an entry tone is played to all connected participants when a participant joins the conference</td>
</tr>
<tr>
<td>Exit Tone</td>
<td>Whether or not an exit tone is played to all connected participants when a participant disconnects from the conference</td>
</tr>
</tbody>
</table>
## Bridge (MCU) Features

The **Bridge (MCU) Features** section, which applies only for conferences that use an MCU, has these fields.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU Name</td>
<td>The MCU device name hosting the conference. Not applicable when the conference is not being hosted on an MCU.</td>
</tr>
<tr>
<td>Numeric ID</td>
<td>The unique conference identifier assigned by the MCU.</td>
</tr>
<tr>
<td>Entry Queue Access</td>
<td>Whether or not the conference has an entry queue enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The Resource Manager system enables entry queues on a per MCU basis and all conferences on an entry queue enabled MCU will be scheduled with entry queue access.</td>
</tr>
<tr>
<td>Meet Me per Conf</td>
<td>Whether or not the conference is a Meet Me conference, for which a dial-in number is assigned, so that undefined participants can connect to the conference</td>
</tr>
<tr>
<td>Message Service Type</td>
<td>Displays the type of messages participants joining the conference hear. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Welcome (No wait)</td>
</tr>
<tr>
<td></td>
<td>• Attended (Wait)</td>
</tr>
<tr>
<td></td>
<td>• IVR</td>
</tr>
<tr>
<td>Message Service Name</td>
<td>Name on the MCU of the Message Service. So, for example, a service name IVR70 which provides the IVR service</td>
</tr>
</tbody>
</table>

### Participants

On the Future and Anytime screens, the list of participants identifies users, rooms, and guests invited to participate. The list on the Ongoing screen identifies participants actively on a call.
### Participant Details

The **Participant Details** section has these fields.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The participant’s name</td>
</tr>
<tr>
<td>Call Info</td>
<td>How the participant joined the call. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Video Dial-Out@&lt;Address&gt;</td>
</tr>
<tr>
<td></td>
<td>• Audio Dial-In</td>
</tr>
<tr>
<td></td>
<td>• Video Dial-In</td>
</tr>
<tr>
<td></td>
<td>• In Person</td>
</tr>
<tr>
<td></td>
<td>• Room Only</td>
</tr>
<tr>
<td>Type</td>
<td>The type of conference connection. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Audio Only</td>
</tr>
<tr>
<td></td>
<td>• Audio-Video</td>
</tr>
<tr>
<td></td>
<td>• Other (for <strong>In Person</strong> and <strong>Room Only</strong> participants)</td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>The name assigned to the participant’s endpoint when added to the system</td>
</tr>
<tr>
<td>Connection Status</td>
<td>The state of the participant’s endpoint connection. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Connected</td>
</tr>
<tr>
<td></td>
<td>• Connecting</td>
</tr>
<tr>
<td></td>
<td>• Declined</td>
</tr>
<tr>
<td></td>
<td>• Disconnected</td>
</tr>
<tr>
<td></td>
<td>• Disconnecting</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• H323</td>
</tr>
<tr>
<td></td>
<td>• ISDN</td>
</tr>
<tr>
<td></td>
<td>• SIP</td>
</tr>
<tr>
<td></td>
<td>• H323_E164</td>
</tr>
<tr>
<td></td>
<td>• H323_ANNEX_O</td>
</tr>
<tr>
<td></td>
<td>• H323_ID</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Address</td>
<td>Used to reach endpoints, such as IP address or E164 number</td>
</tr>
<tr>
<td>Number</td>
<td>The IP address or phone number of the participant's endpoint (if a dial-out) or the participant's port address on the MCU (if a dial-in)</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>The audio or video data transfer rate (in kbps) of the participant's endpoint</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption is either enabled (True) or disabled (False)</td>
</tr>
<tr>
<td>Area</td>
<td>Area or areas assigned to the participant.</td>
</tr>
</tbody>
</table>
Understanding Endpoint Management

This chapter provides an overview on endpoint management and details how to perform many of the Polycom® RealPresence® Resource Manager system endpoint management tasks. It includes these topics:

- “Endpoint Provisioning” on page 73
- “Endpoint Associations and Presence” on page 74
- “Endpoint Software Updates” on page 74
- “Endpoint Passwords” on page 75
- “Standard versus Dynamic Management” on page 75

**Endpoint Provisioning**

Polycom endpoint systems can be configured in three ways:

- In the room by using the system’s remote control to navigate the screens and enter information.
- From a remote location by using the system’s web interface to navigate the screens and enter information.
- From a remote location by using the RealPresence Resource Manager system’s web interface to provision configuration settings to the endpoint system.

The RealPresence Resource Manager system can provision several types of endpoints. Endpoint provisioning, which requires provisioning profiles, allows an administrator to remotely configure multiple endpoints of the same type with a standard set of settings. This eliminates the need to configure each endpoint individually either through the hand-held remote or the endpoint’s web interface.
The RealPresence Resource Manager system supports three types of endpoint provisioning: bundled, automatic, and scheduled. Enable endpoints for only one type of provisioning.

For more information, see:

- “Automatic Provisioning of Endpoints” on page 131
- “Scheduled Provisioning of Endpoints” on page 143
- “Bundled Provisioning of Endpoints” on page 139

Endpoint Associations and Presence

The RealPresence Resource Manager system assumes that users will be associated with endpoints. You can associate a user with more than one endpoint, but one endpoint is designated as the primary endpoint.

When scheduling a user in a conference, the RealPresence Resource Manager system will, by default, schedule the user’s primary endpoint. The scheduler can choose to change the request to schedule one of the user’s other endpoints.

The RealPresence Resource Manager system is also a presence service, which is the part of the system that maintains online status information for the users of dynamically managed endpoints. The presence service allows users to access information about the online status of other users. This is important, because when you make a video call or start a chat, that action only takes you to a endpoint. It doesn’t ensure that you will reach the person you want to reach. The presence service provides information about the user’s availability, which improves your chances of getting the person.

Endpoint Software Updates

The RealPresence Resource Manager system software update feature, which requires a software update profile for the endpoint type and model, allows an administrator to upgrade the software on one or more endpoints with a standard software package. This eliminates the need to upgrade each endpoint individually.

The RealPresence Resource Manager system supports two exclusive software update processes: automatic and scheduled. Automatic and scheduled software update are exclusive endpoint management scenarios. Endpoints enabled for automatic software update should not be scheduled for software updates through the system.

Polycom recommends that all endpoints in a region (that is, a gatekeeper zone) be managed by a single management system.
For more information about updating endpoint software, see “Updating Endpoint and Peripheral Software” on page 101.

**Endpoint Passwords**

A RealPresence Resource Manager system can manage Polycom endpoints only when the password in the device record matches the password in the endpoint. Matching passwords are required to:

- Schedule provisioning of an endpoint through a RealPresence Resource Manager system.
- Use the Scheduled Software Update feature.
- Monitor the endpoint from the **Endpoint > Monitor View**.

You can update the password for certain endpoint systems through scheduled provisioning only after you have entered the matching password in the RealPresence Resource Manager system. In this case, you must instruct end-users not to change the password.

Some companies select an administrative password that is used for all endpoints and regularly updated through provisioning.

For third-party endpoints, passwords may be required to access the endpoint management software.

For information about restrictions in changing passwords for a specific endpoint, see the documentation for the endpoint.

**Standard versus Dynamic Management**

The RealPresence Resource Manager system allows you to manage endpoints in two ways:

- “Standard Management of Endpoints (Polycom and Third-Party)” on page 75
- “Dynamic Management of Endpoints (Polycom Only)” on page 76

**Standard Management of Endpoints (Polycom and Third-Party)**

Standard management allows you to push software updates and provisioning profiles to endpoints at intervals that you define.
Standard management uses server-to-client communication over HTTP. This management technique is more appropriate for corporate networks where both the RealPresence Resource Manager and all endpoints are behind the same firewall.

For more information about standard management methods, see the following:

• “Create Software Updates for Endpoints” on page 102
• “Using Scheduled Software Updates” on page 121

Dynamic Management of Endpoints (Polycom Only)

You can configure a Polycom endpoint to be dynamically managed. Dynamic management is client-to-server over HTTPS which makes it more secure and firewall-friendly.

In dynamic management mode, when an endpoint starts up and at designated intervals thereafter, it automatically polls the RealPresence Resource Manager system for a newer software update package or provisioning profile. If a either is found, the package is sent in XML format over a secure HTTPS connection.

Endpoints do not poll the system if they are in a call. They restart polling after the call ends.

When you do this, you do the following:

1  Configure the DNS server, if you wish it to resolve queries for the RealPresence Resource Manager by the RealPresence Resource Manager’s host name or IP address.

   To dynamically manage endpoints (which includes automatic provisioning, automatic software update, and presence), they must be able to automatically discover the RealPresence Resource Manager. This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager.

2  Configure the endpoint to use the RealPresence Resource Manager as it’s provisioning service.

   You do this via the endpoint’s web interface. You can do this on initial setup or at any time when you need to switch to dynamic management.

3  Set up automatic provisioning on the RealPresence Resource Manager.

   You need to create provisioning profiles for the endpoints you want to automatically provision.

4  Set up automatic software updates on the RealPresence Resource Manager.

   You need to create software updates to automatically send to endpoints.

For more information about dynamic management methods, see the following:
• “Create Software Updates for Endpoints” on page 102
• “Using Automatic Software Updates” on page 106
• “Trial an Automatic Software Update Package” on page 113
• “Automatic Software Updates for Peripherals” on page 116
Managing Endpoints

This chapter provides an overview of the Polycom® RealPresence® Resource Manager system’s endpoint management functions. It includes these topics:

- “Endpoint Menu, Views, and Lists” on page 79
- “Manage Endpoints and Peripherals” on page 85
- “Manage Peripherals” on page 100

## Endpoint Menu, Views, and Lists

The RealPresence Resource Manager system **Endpoint** menu provides these views of the **Endpoint** list:

- **Monitor View** — Displays the list of all registered and managed endpoints. Use this view to monitor and manage endpoints.
- **Peripherals View** — Displays the list of all peripherals connected to managed endpoints. Use this view to see the status of peripherals.
- **Bundled Provisioning** — Displays the list of available endpoint provisioning bundles.
- **Automatic Provisioning** — Displays the list of dynamically managed endpoints eligible for automatic provisioning.
- **Scheduled Provisioning** — Displays the list of standardly managed endpoints eligible for scheduled provisioning.
- **Automatic Software Update** — Displays the list of dynamically managed endpoints eligible for automatic software updates.
- **Scheduled Software Update** — Displays the list of standardly managed endpoints eligible for scheduled software updates.

All of the **Endpoint** views have the following information:
Monitor View

Use the Endpoint Monitor View to monitor and manage endpoints.

Endpoint List in the Monitor View

By default the Endpoint list in the Monitor View displays a list of all endpoints that are registered with the RealPresence Resource Manager system for management and monitoring purposes.
The **Endpoint** list in this view has these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter</strong></td>
<td>Use the filter choices to display other views of the <strong>Endpoint</strong> list, which include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong> - Filters the list by type. For more information, see “<strong>Supported Endpoint Types</strong>” on page 161.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alerts</strong> - Filters the list by alert type: Help, Error, or Warning.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Connection Status</strong> - Filters the list by connection status: In a Call, Online, or Offline.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong> - Filters the list by system name entered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong> - Filters the list by IP address entered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dial String</strong> - Filters the list by dial string (SIP, H.323, or ISDN) entered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Site</strong> - Filters the list by site location entered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Area not the same as Site’s Area</strong> - Available only when Areas are enabled. This filters endpoints that belong to a site which is not</td>
</tr>
<tr>
<td></td>
<td>associated with the area the endpoint belongs to. If the user does not manage the site’s area, he cannot view the Site area information.</td>
</tr>
<tr>
<td></td>
<td>The value for the area will display as “Restricted”.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Area</strong> - Available only when Areas are enabled. Filters the list by the area with which the endpoint is associated. This field is only</td>
</tr>
<tr>
<td></td>
<td>visible when Areas are enabled. You can only view area-specific information for area(s) that you have permission to manage.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VIP</strong> - Filters the list for VIP endpoints.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The state of the endpoint. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Online ☑️</td>
</tr>
<tr>
<td></td>
<td>• Offline ☐️</td>
</tr>
<tr>
<td></td>
<td>• In a call ✅</td>
</tr>
<tr>
<td></td>
<td>• Gatekeeper registered ⬆️</td>
</tr>
<tr>
<td></td>
<td>• Signalling unregistered ⬇️</td>
</tr>
<tr>
<td></td>
<td>• Error 🟢</td>
</tr>
<tr>
<td></td>
<td>• All paired peripherals are connected without alerts ➤</td>
</tr>
<tr>
<td></td>
<td>• One or more paired peripherals are turned off or no longer connected ➤</td>
</tr>
<tr>
<td></td>
<td>• One or more paired peripherals has an error ➤</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>The management mode for the endpoint. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Dynamic management mode 🌠</td>
</tr>
<tr>
<td></td>
<td>• Standard management mode (no icon)</td>
</tr>
<tr>
<td></td>
<td>For a description of these modes, see “<strong>Understanding Endpoint Management</strong>” on page 73.</td>
</tr>
</tbody>
</table>
### Actions in the Monitor View

Besides providing access to the endpoint views, the Actions section of the Monitor View may also include these context-sensitive commands depending on the selected endpoint type.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The assigned name of the endpoint.</td>
</tr>
<tr>
<td>Model</td>
<td>The type of endpoint. For valid endpoint types, see &quot;Supported Endpoint Types&quot; on page 161.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the endpoint.</td>
</tr>
<tr>
<td>Area</td>
<td>(Available only when Areas are enabled.) The area with which the endpoint is associated. Users can only view area information for the areas to which they belong or have been assigned to manage.</td>
</tr>
</tbody>
</table>
| Dial String | The dial string for the endpoint. If the endpoint has more than one dial string, it displays one based on this order:  
  - SIP  
  - H.323  
  - ISDN |
| Site    | The site to which the endpoint belongs.  
  **Note**  
  When areas are enabled on your system, this field shows a value of Restricted if you do not have permission to manage the area to which the site is assigned. |
| Owner   | The user associated with the endpoint. |

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available for all endpoint types</strong></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Manually add an endpoint to the RealPresence Resource Manager system or find a endpoint on the network.</td>
</tr>
<tr>
<td>View Details</td>
<td>Display all of the Device Details for the selected endpoint.</td>
</tr>
<tr>
<td>Edit</td>
<td>Change connection settings for the selected endpoint. Note that if this is a managed endpoint, the endpoint may overwrite settings entered manually.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected endpoints.</td>
</tr>
<tr>
<td>Search Devices</td>
<td>Search the list of endpoints by IP range.</td>
</tr>
</tbody>
</table>
### Action | Use this action to...
--- | ---
**Available for only selected endpoint types**

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage</td>
<td>Open the selected endpoint’s management interface in a separate browser window. This command is not available for the following endpoint types: <strong>iPower, PVX, and Other</strong>.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Send a text message (ASCII only, 100 characters maximum) to the selected endpoint’s video monitor. This command is not available for the following endpoint types: <strong>TANDBERG, iPower, and Other</strong>.</td>
</tr>
<tr>
<td>Clear Help</td>
<td>Clear help for the selected endpoint on the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Reboot Device</td>
<td>Reboot the selected endpoint. This command is only available for <strong>HDX-Series and VSX-Series</strong> endpoints with a <strong>Connection Status of Online</strong>.</td>
</tr>
<tr>
<td>Search Devices</td>
<td>Allows you to search for endpoints within a range of IP addresses. The results message displays the number of endpoints searched and the number of endpoints found within the IP range.</td>
</tr>
<tr>
<td>Manage Owner</td>
<td>Edit information for the user (owner) of the selected endpoint. This command is applicable only when a user is associated with the endpoint.</td>
</tr>
<tr>
<td>View Peripherals</td>
<td>View information about peripherals. This command is only available when one or more peripherals is connected to an <strong>HDX-Series</strong> endpoint.</td>
</tr>
<tr>
<td>Associate User</td>
<td>Manually associate a user with the selected endpoint.</td>
</tr>
<tr>
<td>Assign Area</td>
<td>(Available only when <strong>Areas</strong> are enabled.) Associate the selected endpoint to an area. An endpoint can only be assigned to a user who belongs to the same area as the endpoint. Users can only view area information for the areas to which they have been assigned to manage.</td>
</tr>
</tbody>
</table>

For information about these endpoint actions, see “Understanding Endpoint Management” on page 73.

**Peripherals View**

Use the **Peripherals View** to monitor peripherals connected to dynamically managed endpoints.
## Peripherals List in the Peripherals View

By default the **Peripherals** list displays a list of all peripherals that are connected or have been connected to endpoints managed by the RealPresence Resource Manager system.

The **Peripherals** list in this view has these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Use the filter choices to display other views of the <strong>Endpoint</strong> list, which include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong> - Filters the list by type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Paired HDX</strong> - Filters the list by the HDX to which the peripherals are connected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong> - Filters the list by IP address entered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hardware Version</strong> - Filters the list by hardware version entered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Software Version</strong> - Filters the list by software version entered.</td>
</tr>
<tr>
<td>Status</td>
<td>The state of the peripheral. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Connected</strong> - Peripheral is connected to the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disconnected</strong> - Peripheral is turned off or no longer connected to the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Error</strong> - Endpoint reports an error with the peripheral.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Blank</strong> - Endpoint is not reporting that the peripheral is connected.</td>
</tr>
<tr>
<td>Paired HDX</td>
<td>Name of the endpoint to which the peripheral is connected or <strong>Not Paired</strong>. The <strong>Not Paired</strong> designation means the peripheral was connected to an endpoint, but it is not connected to one now.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of peripheral.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the peripheral.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the peripheral, if applicable.</td>
</tr>
<tr>
<td>Area</td>
<td>(Available only when <strong>Areas</strong> are enabled.) The area with which peripheral is associated. The peripheral inherits its area from the endpoint to which the peripheral is connected. Users can only view area information for the areas to which they belong or have been assigned to manage.</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>The hardware version of the peripheral.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The software version of the peripheral.</td>
</tr>
</tbody>
</table>
**Actions in the Peripheral View**

Besides providing access to the peripherals, the **Actions** section of the **Peripheral View** may also include these context-sensitive commands depending on the selected peripheral type and its status.

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete Peripheral</td>
<td>(Available only when the peripheral is no longer paired with an endpoint.) Delete the peripheral from the <strong>Peripheral View</strong> list.</td>
</tr>
<tr>
<td>Display Applications</td>
<td>(Available only for peripherals on which you can install multiple applications.) Display a list of installed applications and their version.</td>
</tr>
</tbody>
</table>

**Manage Endpoints and Peripherals**

The follow topics describe the actions available in **Endpoint > Monitor View**:

- “View Device Details” on page 86
- “Add an Endpoint or Find an Endpoint on the Network” on page 90
- “Edit an Endpoint” on page 95
- “Delete an Endpoint” on page 95
- “Manage Owner of an Endpoint” on page 96
- “Manage Endpoint” on page 96
- “View an Endpoint’s Video Feed” on page 96
- “Clear an Endpoint Help Request” on page 97
- “Send a Message to an Endpoint” on page 97
- “Reboot an Endpoint” on page 98
- “Associate a User with an Endpoint” on page 98
- “Search for Endpoints in a Range of IP Addresses” on page 98
- “View Peripherals” on page 99
View Device Details

To view detailed information about a managed endpoint

1  Go to Endpoint > Monitor View.
2  As needed, use the Filter to customize the endpoint list.
3  Select the endpoint of interest and click View Details.

The Device Details dialog box displays the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Endpoint names must be unique.</td>
</tr>
<tr>
<td></td>
<td>• The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid.</td>
</tr>
<tr>
<td></td>
<td>• The system name might be different than the H.323 ID.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of endpoint. For valid types, see “Supported Endpoint Types” on page 161.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The assigned IP address of the endpoint.</td>
</tr>
<tr>
<td>DNS Name</td>
<td>The DNS name (FQDN) of the endpoint.</td>
</tr>
<tr>
<td>Owner</td>
<td>The person to whom the endpoint is assigned.</td>
</tr>
<tr>
<td>Site</td>
<td>The network site for the endpoint. By default, endpoints are added to the Primary Site.</td>
</tr>
</tbody>
</table>

**Note**
When areas are enabled on your system, this field shows a value of Restricted if you do not have permission to manage the area to which the site is assigned.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A free-form text field (extended ASCII only) in which information about the endpoint can be added.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number (ASCII only) of the endpoint. The endpoint provides the serial number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed.</td>
</tr>
</tbody>
</table>
### Field Description

**HTTP URL**
The management URL for the endpoint, if available (ASCII only). This URL allows the RealPresence Resource Manager system to start the endpoint's management system using the Manage function.

All Polycom endpoints allow management through a browser. For these endpoints, this field is completed when the endpoint registers with the RealPresence Resource Manager system.

**HTTP Port**
The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.

**Area**
The area to which the endpoint is assigned.
This field is only visible when Areas are enabled.
A user can only view area-specific information for an area(s) that he has permission to manage.

**Addresses**

**SIP URI**
A SIP URI is the address used to call another person via SIP. In effect it's a user’s SIP phone number. The SIP URI will be of the following format:

\(<username>@host(domain or IP):Port\)

**Aliases**
The aliases that allow you to connect to the endpoint.
The RealPresence Resource Manager system converts the aliases to the IP address associated with the endpoint.

- **Alias Type**. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown.
- **Alias Value**. Value for the alias type shown.
- The endpoint name is the system name, which might be different from the H323 ID.
- The value of the E.164 alias is the extension dialed to reach this endpoint.

**Notes**
- To add aliases for the endpoint, edit the endpoint.
- The following **Alias Values** are ASCII only: H323 ID, URL, Transport Address, and Unknown.

**ISDN Video Number**
For ISDN endpoints only, the country code + city/area code + phone number for the endpoint.
When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. Only native ISDN is supported.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Host Name</td>
<td>The host name of the endpoint on the LAN. This can be different from the system name of the endpoint. It is an ASCII only name.</td>
</tr>
<tr>
<td>Call Signaling Address</td>
<td>The port on which the gatekeeper associated with the RealPresence Resource Manager system sends call signaling information.</td>
</tr>
<tr>
<td>RAS Address</td>
<td>The port on which the gatekeeper associated with RealPresence Resource Manager system sends RAS addressing information.</td>
</tr>
<tr>
<td><strong>Capabilities</strong></td>
<td></td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>The communications protocols that the endpoint can support. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP (H.323)</strong> - A standard that defines the protocols used for multimedia communications on packet-based H.323 networks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP (SIP)</strong> - A standard that defines the protocols used for multimedia communications on SIP networks.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ISDN (H.320)</strong> - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.</td>
</tr>
<tr>
<td></td>
<td>For endpoints with the type Unknown, select H.323. The endpoint automatically provides the protocols if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Required MCU Service</td>
<td>The MCU service selected for the endpoint to use.</td>
</tr>
<tr>
<td>Capabilities Enabled</td>
<td>Capabilities enabled on this endpoint. Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>MCU</strong> - The endpoint can act as a control unit for multipoint conferences</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gateway</strong> - The endpoint can act as a gateway for call management</td>
</tr>
<tr>
<td></td>
<td>The MCU provides the capability if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Monitoring Level</td>
<td>The monitoring level for the endpoint. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Standard</strong>. This endpoint is monitored.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VIP</strong>. This endpoint is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.</td>
</tr>
<tr>
<td>Available to Schedule</td>
<td>Identifies if the endpoint is available when users are scheduling conferences.</td>
</tr>
</tbody>
</table>
### Call Info > Sites

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Far Site Name</td>
<td>The H.323 ID of the far site endpoint to which the selected endpoint is connected. When multiple endpoints are connected through the endpoint's embedded MCU, this field displays a concatenation of each endpoint's H.323ID separated by '</td>
</tr>
<tr>
<td>Far Site Number</td>
<td>The address of the far site endpoint to which the selected endpoint is connected. The address value for the calling endpoint appears to be the dialed address. The address value for the called endpoint appears to be the IP Address.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The type of encryption the far site uses.</td>
</tr>
<tr>
<td>Cause Code</td>
<td>The cause code showing how the call ended.</td>
</tr>
<tr>
<td>Error</td>
<td></td>
</tr>
<tr>
<td>Video FEC Errors</td>
<td>The number of Forward Error Correction (FEC) errors that have been corrected in the current call.</td>
</tr>
</tbody>
</table>

### Call Info > Call Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Protocol</td>
<td>The video connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• H.261 H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions.</td>
</tr>
<tr>
<td></td>
<td>• H.263 H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions.</td>
</tr>
<tr>
<td></td>
<td>• H.264</td>
</tr>
<tr>
<td>Video Format</td>
<td>The video format, both transmission (Tx) and reception (Rx), the endpoint is using.</td>
</tr>
<tr>
<td>Video Rate</td>
<td>The video bandwidth negotiated with the far site.</td>
</tr>
<tr>
<td>Video Rate Used</td>
<td>The actual video bandwidth used in the call to the far site.</td>
</tr>
<tr>
<td>Video Frame Rate</td>
<td>Specifies the frame rate the endpoint is using.</td>
</tr>
</tbody>
</table>
## Add an Endpoint or Find an Endpoint on the Network

This topic describes how to manually add endpoints and how to find endpoints on the same network as the system.

For most endpoints, you enter basic information. The system then locates the endpoint and retrieves its information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Protocol</td>
<td>The audio connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• G.711</td>
</tr>
<tr>
<td></td>
<td>• G.722</td>
</tr>
<tr>
<td></td>
<td>• G.728</td>
</tr>
<tr>
<td>Audio Rate</td>
<td>The audio bandwidth negotiated with the far site</td>
</tr>
</tbody>
</table>

### Call Info > Quality of Service (Not reported by all endpoint types)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Packet Loss</td>
<td>Specifies the total packet loss for the currently active call that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.</td>
</tr>
<tr>
<td>% Packet Loss</td>
<td>Specifies the average percentage of packet loss for the currently active call that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.</td>
</tr>
<tr>
<td>Audio Packet Loss</td>
<td>Specifies the audio packet loss for the currently active call.</td>
</tr>
<tr>
<td>Video Packet Loss</td>
<td>Specifies the video packet loss for the currently active call.</td>
</tr>
<tr>
<td>Audio Jitter</td>
<td>Specifies the audio jitter for the currently active call.</td>
</tr>
<tr>
<td>Video Jitter</td>
<td>Specifies the video jitter for the currently active call.</td>
</tr>
</tbody>
</table>

### Call Info > Video Feed

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Near Site</td>
<td>The video feed from the endpoint.</td>
</tr>
<tr>
<td>Far Site</td>
<td>The video feed from the endpoint to which the endpoint is connected.</td>
</tr>
</tbody>
</table>

### System Alerts

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>Endpoint error message, for example, GK Registration error.</td>
</tr>
<tr>
<td>Warnings</td>
<td>Endpoint warning message, for example, Low Battery.</td>
</tr>
</tbody>
</table>
When a SIP-only endpoint registers with the Polycom DMA system and does not register with the RealPresence Resource Manager system’s provisioning service to become dynamically managed, you must manually add it to the RealPresence Resource Manager system in order to manage that endpoint.

To add an endpoint to the system or find an endpoint on the network

1. Go to Endpoint > Monitor View and click Add.
2. In the Add New Device dialog box, select the Device Type. For valid types, see “Supported Endpoint Types” on page 161. For endpoints not specified in the list, select a Device Type of Other.
3. Enter the IP Address of the endpoint.
4. Click Find Device.
   - If the RealPresence Resource Manager system can find the endpoint on the network, the Add New Device dialog box is populated with information retrieved from the endpoint. Review any information retrieved from the endpoint.
   - If the RealPresence Resource Manager system cannot find the endpoint on the network, a Device Not Found dialog box appears.

If you enter an invalid Admin ID or Password for an endpoint that requires that information, the RealPresence Resource Manager system may still find the endpoint. It depends upon the endpoint type.

- Polycom HDX systems won’t allow the RealPresence Resource Manager system to detect the endpoint type and complete the registration. You can manually add the endpoint, but the RealPresence Resource Manager system cannot communicate with it until you’ve entered a valid Admin ID or Password for the endpoint. In this case, the RealPresence Resource Manager system records an error message in an error log.
- The Find Device function only works for endpoints with a specified Device Type. If you selected a Device Type of Other, the RealPresence Resource Manager system will report an error.

5. Assign the endpoint a System Name.
   Endpoint names must be unique, must be in ASCII only, and may have an unlimited number of characters. Spaces, dashes, and underscores are valid.

6. If necessary, enter the Admin ID and Password for the endpoint. Some endpoints may not require this information. Other endpoints may require only a password.
Complete the **Identification**, **Addresses**, and **Capabilities** sections of the **Add New Device** dialog box.

Pay particular attention to the **Capabilities** options, because these settings determine how the endpoint is used throughout the RealPresence Resource Manager system. For example, you can select it as a VIP endpoint and determine whether it will be **Available to Schedule** through the scheduling interface.

Note that many fields in this dialog box are ASCII only. Depending on the selected type, some of these fields may not be displayed or may not be editable.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification</strong></td>
<td><strong>Description</strong> A free-form text field (extended ASCII only) in which information about the endpoint can be added.</td>
</tr>
<tr>
<td><strong>GAB Display Name</strong></td>
<td>Enter a name for the endpoint as it will appear in the Global Address Book.</td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>The network site for the endpoint. The system determines the site based upon IP address.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When areas are enabled on your system, this field shows a value of <strong>Restricted</strong> if you do not have permission to manage the area to which the site is assigned.</td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
<td>The serial number (ASCII only) of the endpoint. The endpoint provides the serial number if it registered successfully or is managed.</td>
</tr>
<tr>
<td><strong>Software Version</strong></td>
<td>The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed.</td>
</tr>
<tr>
<td><strong>HTTP URL</strong></td>
<td>The management URL for the endpoint, if available (ASCII only). This URL allows the RealPresence Resource Manager system to start the endpoint 's management system using the <strong>Manage</strong> function. All Polycom endpoints allow management through a browser. For these endpoints, this field is completed when the endpoint registers with the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td><strong>HTTP Port</strong></td>
<td>The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.</td>
</tr>
</tbody>
</table>
### Assign Area

Assign this endpoint to an area. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage. Users with area roles are required to assign the endpoint to an area. If the user manages only one area, the endpoint will automatically be assigned to that area.

### Addresses

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Name</td>
<td>The name for the endpoint as entered on the domain name server.</td>
</tr>
<tr>
<td>SIP URI</td>
<td>The address used to call the endpoint via SIP. <code>&lt;username&gt;@host(domain or IP):Port</code></td>
</tr>
</tbody>
</table>

### Aliases

The aliases that allow you to connect to the endpoint. The RealPresence Resource Manager system converts the aliases to the IP address associated with the endpoint.

- **Alias Type.** Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown.
- **Alias Value.** Value for the alias type shown.

### Notes

- The following **Alias Values** are ASCII only: **H323 ID**, **URL**, **Transport Address**, and **Unknown**.
- In other cases, the endpoint name is the system name, which might be different from the H323 ID.
- The value of the E.164 alias is the extension dialed to reach this endpoint.

### ISDN Video Number

For ISDN endpoints only, the country code + city/area code + local phone number for the endpoint. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The RealPresence Resource Manager system only supports native ISDN.
Click Add.

The endpoint appears in the Endpoint list. By default, the system may also:

- Add the endpoint to the applicable site.
- Set the HTTP Port to 80
- Add an Alias for the endpoint.
- Make the endpoint Available to Schedule
- Set the Monitoring Level to Standard
Once you’ve added an endpoint, you can associate it with a user. See “Assign Users Roles and Endpoints” on page 292.

Edit an Endpoint

The system automatically detects IP address changes and updates its database with the new information for Polycom and third-party endpoints that are registered with the RealPresence Resource Manager system.

To edit an endpoint in the RealPresence Resource Manager system
1. Go to Endpoint > Monitor View
2. As needed, use the Filter to customize the endpoint list.
3. Select the endpoint of interest and click Edit.
4. As required, edit the Identification, Addresses, and Capabilities sections of the Edit Device dialog box. For more information, see “View Device Details” on page 86.
   Note that many fields in this dialog box are ASCII only.
5. Click Update.

Deleting information for an endpoint on the RealPresence Resource Manager system does not change the information in the endpoint. To make changes in the endpoint information, use Provisioning or change it at the endpoint interface. Note that for managed endpoints, the endpoint may overwrite settings entered manually.

Delete an Endpoint

To delete an endpoint from the RealPresence Resource Manager system
1. Go to Endpoint > Monitor View
2. As needed, use the Filter to customize the endpoint list.
3. Select the endpoint of interest and click Delete.
4. Click Yes to confirm the deletion.
   The Endpoint list is updated.
Manage Owner of an Endpoint

To manage the owner (user associated with the endpoint) of an endpoint

1. Go to Endpoint > Monitor View.
2. As needed, use the Filter to customize the Endpoint list.
3. Select the endpoint of interest and click Manage Owner.
   The Edit User dialog box appears.
4. Edit any user properties you need.
5. Click OK.

Manage Endpoint

You can navigate to the management interface of an endpoint from the RealPresence Resource Manager.
This function is not available for all endpoint types.

To manage an endpoint from the RealPresence Resource Manager system

1. Go to Endpoint > Monitor View
2. As needed, use the Filter to customize the Endpoint list.
3. Select the endpoint of interest.
4. Click Manage.
   A new browser instance opens and navigates to the web interface of the

View an Endpoint’s Video Feed

This procedure is available on the following endpoint types:
- Polycom HDX system
- TANDBERG
- VSX-Series

To view the video feed for an endpoint (near site or far site)

1. Go to Endpoint > Monitor View.
2. As needed, use the Filter to customize the Endpoint list.
3. Select the endpoint of interest and click View Details.
The Device Details dialog box appears. For information about these fields, see “View Device Details” on page 86.

4 Click Call Info to expand the Call Info options and select Video Feed. The Endpoint Video section shows the video feed from the near and far site.

### Clear an Endpoint Help Request

**To clear an endpoint help request from the RealPresence Resource Manager system**

1 Go to Endpoint > Monitor View
2 As needed, use the Filter to customize the Endpoint list.
3 Select the endpoint of interest and click Clear Help.
   - The Confirm Endpoint Help Clear dialog box appears.
4 To send a message to the endpoint as well as clear the help request, check Also send message to endpoint.
5 Click Clear.
6 If you selected the Also send message to endpoint check box, enter the text message to send the endpoint in the Send Message to Endpoint dialog box and click Send.
   - The Endpoint list is updated and alerts for the endpoint are cleared.

If the reason for the original alert still exists on the endpoint, the alert will likely reappear in the Endpoint list.

### Send a Message to an Endpoint

In some situations, such as in response to a help request, you can send a message to some types of endpoints.

**To send a message to an endpoint from the RealPresence Resource Manager system**

1 Go to Endpoint > Monitor View
2 As needed, use the Filter to customize the Endpoint list.
3 Select the endpoint of interest.
   - If the endpoint can receive text messages, a Send Message option appears in the Action menu.
4 Click Send Message.
5 In the Send Message to Endpoint dialog box, enter a text message and click Send.

The message is sent to the endpoint.

Reboot an Endpoint

In some situations, for example when a remote endpoint is unresponsive, you may need to reboot an endpoint remotely through the RealPresence Resource Manager system.

To reboot an endpoint from the RealPresence Resource Manager system
1 Go to Endpoint > Monitor View
2 As needed, use the Filter to customize the Endpoint list.
3 Select the endpoint of interest.
4 Click Reboot Device.
5 To confirm the request, click Reboot.

Associate a User with an Endpoint

To associate an endpoint to a user within the RealPresence Resource Manager system
1 Go to Endpoint > Monitor View
2 As needed, use the Filter to customize the Endpoint list.
3 Select the endpoint of interest.
4 Click Associate User.
5 In the Last Name field of the Associate User dialog box, enter all or part of the user’s last name and click Search.

The system displays the list of users who meet your search criteria.
6 Select the user of interest and click Close.

Search for Endpoints in a Range of IP Addresses

To search for a set of endpoints within a range of IP addresses
1 Go to Endpoint > Monitor View and click Search Devices.
2 In the **Search Devices** dialog box, enter the starting IP address and ending IP address for the search range and click **Search**.

The system begins searching for endpoints. A progress bar displays the status of the search and a results message displays the number of endpoints searched and the number of endpoints found within the IP range.

**View Peripherals**

If an endpoint has one or more peripherals connected, you can view information about the peripherals.

1 Go to **Endpoint > Monitor View** and select an endpoint that has peripherals connected.

2 Click **View Peripherals**.

3 From the **Peripherals** dialog box, select the peripheral of interest to see the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paired HDX</td>
<td>Name of the HDX the peripheral is connected to.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the peripheral.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the peripheral, if applicable.</td>
</tr>
<tr>
<td>Area</td>
<td>The area in which the peripheral is associated. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>Version of the peripheral hardware.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Version of the peripheral software.</td>
</tr>
<tr>
<td>Pairing Status</td>
<td>The status can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Connected</td>
</tr>
<tr>
<td></td>
<td>• Disconnected</td>
</tr>
<tr>
<td>Alert Status</td>
<td>Alert status of the peripheral, if applicable. Not all peripherals report an alert status.</td>
</tr>
<tr>
<td>Area</td>
<td>The area to which the peripheral belongs. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.</td>
</tr>
</tbody>
</table>
Manage Peripherals

The following topics describe the actions available in the Endpoint > Peripherals View:

- Delete Peripheral
- Display Applications

Delete Peripheral

You can delete peripherals from the Peripherals View list when the peripheral is no longer connected to an endpoint.

1. Go to Endpoint > Peripherals View and select a peripheral that is listed as Not Paired.
2. Click Delete Peripheral.
3. In the Confirm Delete dialog box, click Yes.

Display Applications

For peripherals on which you can install multiple applications, you can display a list of installed applications and their version.

1. Go to Endpoint > Peripherals View and select a peripheral.
2. Click Display Applications.
   The Applications Installed on dialog box for the selected peripheral appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Name of the peripheral application.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the peripheral application.</td>
</tr>
</tbody>
</table>

3. Click Close.
The Polycom® RealPresence® Resource Manager system software update feature, which requires a software update profile for the endpoint type and model, allows an administrator to upgrade the software on one or more endpoints with a standard software package. This eliminates the need to upgrade each endpoint individually.

The RealPresence Resource Manager system supports two exclusive software update processes: automatic and scheduled. Automatic and scheduled software update are exclusive endpoint management scenarios. Endpoints enabled for automatic software update should not be scheduled for software updates through the system.

Polycom recommends that all endpoints in a region (that is, a gatekeeper zone) be managed by a single management system.

This chapter describes how to use Polycom® RealPresence® Resource Manager system to update the software on Polycom endpoints when a new software package is available. It includes these sections:

- “Software Update Considerations for Multi-Tenancy” on page 102
- “Create Software Updates for Endpoints” on page 102
- “Using Automatic Software Updates” on page 106
- “Trial an Automatic Software Update Package” on page 113
- “Automatic Software Updates for Peripherals” on page 116
- “Using Scheduled Software Updates” on page 121
Software Update Considerations for Multi-Tenancy

Within a multi-tenancy environment, area administrators are not allowed to create software updates or set up maintenance windows for automatic software updates. However, they are allowed to schedule software updates that have already been uploaded by a user with the administrator role.

Software update images are also not area-aware, which means that users with area administrator roles see all software updates on the system, not just those for their area. As a best practice, the system administrator should either name the software update appropriately or add information to the description field of the update so that area administrators know which updates to use for their area.

Create Software Updates for Endpoints

To implement an automatic or scheduled software update, you must first create respective software updates for your endpoints.

These tasks must be performed regardless of which type of software update you want to use. Keep in mind that software updates are stored according to the method you use to update the software.

Only users with the administrator role can create software updates.

You must create automatic software updates using the Admin > Automatic Updates menu and you must create scheduled software updates using the Admin > Scheduled Update menu.

A default automatic software update profile—with the description **CMA Desktop - shipped version**—is available for the CMA Desktop client. Default software update profiles are not available for other endpoint systems.

To create a software update, perform this series of tasks.

1. “List the Serial Numbers for the Endpoints to be Updated” on page 103.
2. “Download the Required Software Package” on page 104.
4. “Upload the Software Update” on page 106. For more information on software update profiles, see “View Automatic Software Update Information for an Endpoint” on page 110.
List the Serial Numbers for the Endpoints to be Updated

To list the serial numbers for the endpoints to be updated:

1. Go to Admin > Software Updates > Automatic Software Updates or Admin > Software Updates > Scheduled Software Updates. Be sure to create the update using the menu option corresponding to the method you wish to use: automatic or scheduled.

   The automatic software update feature is only available for these endpoint types:
   • Polycom HDX system endpoints deployed in dynamic management mode
   • Polycom CMA Desktop systems

2. Select the appropriate Endpoint Type and Endpoint Model combination for the endpoint to update. You can select more than one Endpoint.

3. Click Get Serial Numbers.

   The Endpoint Serial Number List appears listing the endpoints of the selected type and model that are eligible for software updates.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the endpoint system</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the endpoint.</td>
</tr>
<tr>
<td>Version</td>
<td>The current software version installed on the endpoint.</td>
</tr>
<tr>
<td>Site</td>
<td>The site to which the endpoint belongs.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>When areas are enabled on your system, this field shows a value of Restricted if you do not have permission to manage the area to which the site is assigned.</td>
</tr>
<tr>
<td>Area</td>
<td>(Available only when Areas are enabled.) The area with which the endpoint is associated. Users can only view area information for the areas to which they belong or have been assigned to manage.</td>
</tr>
</tbody>
</table>

4. As needed, use the Filter to customize the endpoint list.

5. Select the specific endpoints to be updated. To select all endpoints in the list, click the check box in the column header.
6 Click **Get Serial Numbers**.
The serial number(s) appear in the text box on the page.

7 When updating a single endpoint:
   a Record the serial number: ______________________________________
   b Click **Close**.
      The **Software Updates** list reappears.

8 When updating multiple endpoints:
   a Copy and paste the serial numbers from the endpoint serial number list to a .txt file that you can submit to the **Polycom Product Activation** site. Put one serial number per line as shown in the following example.
      82U/1U0/1D1U1U
      82070407E010CD
      820418048078B2
      82040903E00FB0
   b Return to the endpoint serial number list and click **Close**.
      The **Software Updates** list reappears.
   c Repeat steps 2 through 8 for the each endpoint or set of endpoints to be updated. You may include all of the serial numbers for all of the different endpoint types in the same .txt file.
   d Save the .txt file.

**Download the Required Software Package**

To **download the software package required to update the endpoints**

1 On your local system, create a directory to which to save the software package (if one does not already exist).

2 For Polycom endpoints:
   a Open a web browser and go to http://support.polycom.com.
   b In the **Downloads** section, select the **Product** and **Category** for the required software package.
   c Select the software package and save it to the directory created in step 1.
   d Repeat steps a through c for each endpoint type to be updated. Note that the software package may contain the software for different models of the same endpoint type.
3 For third-party endpoints, follow the company’s recommended procedure for downloading a software package. Save it to the directory created in step 1.

**Request Update Activation Keys**

**To request upgrade activation keys**

1 For Polycom products
   a Go to [http://support.polycom.com](http://support.polycom.com).
   b Log in or Register for An Account.
   c Select Product Activation.
   d In the Software Upgrade Key Code section, click Retrieve Software KeyCode.
   e When upgrading a single endpoint:
      » Enter the serial number of the endpoint to be updated into the Serial Number field of the Single Upgrade Key Code section.
      » Enter the version number to which you are upgrading and click Retrieve.
      » The key code is returned on the screen.
      » Record the key code and create a .txt file with the Serial Number - Key Code combination to be updated.
      » Close the Product Activation screens.
   f When updating multiple endpoints from a prepared .txt file (step 8 on page 104):
      » In the Multiple Upgrade KeyCode section, click Add Attachment.
      » Browse to the location of the .txt file you created in step 8 on page 104 and click Upload.
      » A file containing the Serial Number - Key Code combinations will be E-mailed to the specified E-mail account.
      » When you receive the .txt file, save it to your local system.
      » Close the Product Activation screens.

2 For third-party endpoints, follow the company’s recommended procedure for requesting an upgrade activation key.
Upload the Software Update

To upload the software package and create an automatic software update profile

1. Go to Admin > Software Updates > Automatic Software Updates or Admin > Software Updates > Scheduled Software Updates.

2. Click Upload Software Update.

3. In the Upload Software Update dialog box, verify the endpoint type and model.

4. If an activation key code is required to activate the software update, click Update Requires Key and in the Software Update Key File field browse to the .txt key file (received in “Request Update Activation Keys” on page 105).

5. In the Software Update File field, browse to the software update file you downloaded.

6. Enter a meaningful description that will help other users to understand the purpose of the software update.

7. Click OK.

A software update profile for the endpoint type and model type is created.

Using Automatic Software Updates

Automatic software update, which controls the endpoint’s software version level, is tied to the endpoint type. Currently, the automatic software update feature is only available for these endpoint types.

- Polycom HDX system endpoints deployed in dynamic management mode
- Polycom CMA Desktop systems
- Polycom VVX systems
- Polycom Touch Controls

In dynamic management mode, when a endpoint starts up and at designated intervals thereafter, it automatically polls the RealPresence Resource Manager system for a newer software update package. If a software update is necessary, the package is sent in XML format over a secure HTTPS connection.
Endpoints do not poll for software update packages if they are in a call. They restart polling after the call ends.

This section describes how to use the RealPresence Resource Manager system to automatically update the software on Polycom endpoints when a new software package is available. It includes these sections:

- “Set an Automatic Software Update Policy” on page 107
- “Automatic Software Update View” on page 108
- “View Automatic Software Update Information for an Endpoint” on page 110
- “View Automatic Software Update Packages” on page 112
- “Set Maintenance Window for Automatic Software Updates” on page 113

Set an Automatic Software Update Policy

After creating an automatic software update, you can use the Version to use and Allow this version or newer selections to manage the roll out of software update packages. These selections also allow you to manage the release of multiple software packages for the same endpoint type.

Here’s how it works: All endpoints have a current version of software. To automatically overwrite that current software with a different software version on all dynamically managed endpoint systems:

1. You first create a new automatic software update.
2. Then to activate the roll out, you change the Version to use selection from the current value (None by default) to the new version number and Update the page.

The next time a dynamically managed endpoint polls the RealPresence Resource Manager system, it will detect that it has a different software version than the Version to use selection, so it will automatically download and install the identified software update package. Use this method to force users to use a specific software version.

If you also enable the Allow this version or newer selection, anytime upload a newer version of software into an automatic software update that update will be automatically installed on all dynamically managed endpoint systems.

Some important things to note about software versions

- Newer software is identified by the version number. If the Allow this version or newer selection is enabled, when a dynamically managed endpoint polls the RealPresence Resource Manager system, the system
will compare the current software version number with the packaged software version numbers. The RealPresence Resource Manager system will send the software package with the highest version number to the endpoint.

- You can also use the **Version to use** selection to roll endpoints back to older software versions. If you change the **Version to use** selection to an older software version and clear the **Allow this version or newer** selection, the RealPresence Resource Manager system will send the specifically identified software package to the endpoint even if it is an older version.

To roll back a Polycom CMA Desktop client to an older version, you must first remove the existing Polycom CMA Desktop client via the Windows **Add or Remove Software** selection. Then you can install the older software package.

To set an automatic software update policy for an endpoint type

1. Go to **Admin > Software Updates > Automatic Software Updates**.
2. Select the tab for the endpoint type of interest.
3. Choose one of these policies:
   - To specify an area to which to apply the update, use the **Select Area** drop-down to select the area to apply the policy. This feature is only available when areas are enabled and you manage more than one area.
   - To specify a minimum version of automatic software update package, make that version the **Version to use** and select **Allow this version or newer**.
   - To require a specific version of automatic software update package, make that version the **Version to use** and clear **Allow this version or newer**.
   - To turn automatic software update off for an endpoint type, change the **Version to use** value to **(none)**.
4. Click **Update**.

**Automatic Software Update View**

Use the **Endpoint > Automatic Software Update** menu to view the list of endpoints that have registered to the system for automatic software updates.
### Endpoint List in the Automatic Software Update View

By default the Endpoint list in the Automatic Software Update View displays all endpoints eligible for automatic software update. It has the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Filter | Filter choices for this view include:  
  - **Type**—Filters the list by endpoint type.  
  - **Name**—Searches the list by the endpoint’s system name.  
  - **IP Address**—Searches the endpoint list by IP address.  
  - **ISDN Video Number**—Searches the endpoint list by ISDN video number.  
  - **Dial String**—Searches the endpoint list by dial string (SIP, H.323, or ISDN).  
  - **Site**—Searches the endpoint list by site location.  
  - **Area**—Filters the endpoint list by area. This filter is only available when areas are enabled and when the user manages more than one area. |
| Status | The status of the endpoint’s last software update. Possible values include:  
  - **Success**  
  - **Failed**  
  - **Clear** |
| Name | The system name of the endpoint. |
| Type | The type of endpoint. Automatic software update is only available for these endpoint types:  
  - **All**—Displays all dynamically managed systems together.  
  - **HDX Series**—Displays just the Polycom HDX systems deployed in dynamic management mode.  
  - **CMA Desktop**—Displays just the Polycom CMA Desktop systems.  
  - **VVX**—Displays just the Polycom VVX systems. |
| IP Address | The IP address assigned to the endpoint. |
| Area | (Available only when **Areas** are enabled.) The area with which the endpoint is associated. You can only view area information for the areas you have been assigned to manage. If you do not manage more than one area, this column is not displayed. |
View Automatic Software Update Information for an Endpoint

To view information for endpoints that are eligible for automatic software updates

1. Go to Endpoint > Automatic Software Update.
   The Automatic Software Update page appears.

2. As needed, use the Filter to customize the endpoint list. Filter choices include Type, Name, IP Address, ISDN Video Number, Alias, Site and Area.

3. Select the endpoint of interest.

4. In the right pane, expand the Software Update Details tab.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Software Update Status        | The device’s software update status. Possible values include:  
  • Clear. A software update has not been done.  
  • Pending. A software update has been scheduled and is pending. The device may be offline or in a call.  
  • In Progress. The software update is in progress.  
  • Success. A software update has completed successfully.  
  • Failed. A software update could not be performed. |
| Scheduled                     | For automatic updates, this value is N/A.  
For scheduled updates, the date and time, in the default format of yyyy-mm-dd hh:mm, when the device software is schedule to be updated.  
This field is blank if the device is not scheduled for provisioning. |
| Last Attempt Date/Time        | The date and time, in the default format of yyyy-mm-dd hh:mm:ss, of the last software update message exchanged with the device. |
| Failure Reason                | A text description of the reason the software update failed. Causes for failure may include:  
  • The software update file location does not exist.  
  • A password for the device is set in the video endpoint system, and you must enter it in RealPresence Resource Manager system.  
  • A network error has occurred.  
  • The update has timed out.  
  • An internal error occurred on the device, and you must reboot it.  
  • A profile has not been configured.  
  • An endpoint is offline.  
  • An incorrect activation key is in the key file.  
  • An unknown error has occurred. Reboot the device |
| Log Message                   | A read-only text box that contains the log message text recorded during the execution of the software update.  
Note that there are no log messages displayed for dynamically-managed endpoints. |

For more information, see “Software Update Details” on page 220.
View Automatic Software Update Packages

To view the list of automatic software update packages

1 Go to Admin > Software Updates > Automatic Software Updates.

The Automatic Software Updates page appears and the Polycom HDX Series automatic software update packages are displayed. The Automatic Software Updates page includes this information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Area</td>
<td>Allows you to specify an area to which to apply the update.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>The type of endpoint system. You can use automatic software updates for the following Polycom endpoints and peripherals:</td>
</tr>
<tr>
<td></td>
<td>• HDX Series</td>
</tr>
<tr>
<td></td>
<td>• CMA Desktop (PC and Mac OS)</td>
</tr>
<tr>
<td></td>
<td>• VVX</td>
</tr>
<tr>
<td></td>
<td>• Polycom Touch Control</td>
</tr>
<tr>
<td>Version to use</td>
<td>Displays the default automatic software update profile to be used for the endpoint type and model.</td>
</tr>
<tr>
<td>Allow this version or newer</td>
<td>When checked, indicates that when a newer automatic software update package for the endpoint type and model is added, that package should be used as the default package.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the software package associated with the automatic software update package.</td>
</tr>
<tr>
<td>Description</td>
<td>The meaningful name given to the automatic software update package when it was created.</td>
</tr>
<tr>
<td>Uploaded</td>
<td>The date and time when the automatic software update package was created.</td>
</tr>
<tr>
<td>Trial Group</td>
<td>The trial group assigned to the software update package, if applicable.</td>
</tr>
</tbody>
</table>

2 To view the automatic software update packages for other endpoints and peripherals, click the appropriate tab: **CMA Desktop (PC)**, **CMA Desktop (Mac)**, **VVX** or **Polycom Touch Control**.
Set Maintenance Window for Automatic Software Updates

You can restrict automatic software updates of dynamically-managed HDX endpoint systems to a scheduled maintenance window.

Typically, automatic software updates occur as specified by the Software Update Polling Interval (Admin > Site > Edit Site Provisioning Details > Provisioning Settings). Enabling the maintenance window feature in the RealPresence Resource Manager system overrides the Software Update Polling Interval. The RealPresence Resource Manager system provisions the maintenance window to the HDX systems, and the endpoints hold their automatic software update requests until the maintenance window starts.

Some notes about this feature:

- It applies to dynamically-managed HDX systems only.
- To avoid automatically updating the software on all HDX systems at the start of the maintenance window, the HDX systems randomize their automatic software update requests.

To restrict automatic software updates to a scheduled maintenance window

1. Go to Admin > Software Update > Automatic Software Update > Maintenance Window.
2. In the Maintenance Window dialog box, click Enable Maintenance Window and set a maintenance window Start Time and either an End Time or Duration.

Set the maintenance window start time to the HDX system local time, not the RealPresence Resource Manager system local time. For example, if you set the maintenance window start time to 3am, the maintenance window for each HDX system will start at 3am local time. Therefore, the maintenance window for HDX systems in Buffalo, NY will start at 3am EST; the maintenance window for HDX systems in Denver, CO will start at 3am MST; and the maintenance window for HDX systems in San Francisco, CA will start at 3am PST.

3. Click Save.

Trial an Automatic Software Update Package

Setting up a trial of a software update requires the user to update a software update. Only users with the administrator role can do this. Users with the area administrator role cannot upload software updates.
**To trial a software update package:**

1. Get the things you need to create the package. You must have the administrator role to complete the tasks in this step:
   - a. “List the Serial Numbers for the Endpoints to be Updated” on page 103.
   - b. “Download the Required Software Package” on page 104.
   - c. “Request Update Activation Keys” on page 105.

2. Set up testing. Complete these tasks:
   - a. “Create a Local Trial Group” on page 114.
   - b. “Upload the Software Package and Create a Trial Software Update Package” on page 114. For more information on software update packages, see “View Automatic Software Update Information for an Endpoint” on page 110.

3. Once your testing of the trial software package is complete, do one of these tasks:
   - “Promote the Trial Software Update Package to Production” on page 115
   - “Delete the Trial Software Update Package” on page 116.

**Create a Local Trial Group**

To trial a software update with a specific group of local and/or enterprise users, create a local group that includes these users, as described in “Add a Local Group” on page 289. The people in this group will receive the trial software update package when their endpoint goes through its normal, automated software update process.

- You can use an existing enterprise group as a trial group, but you will not be allowed to change the enterprise group in any way.
- If the trial software group is a parent group with children, all of its children will inherit trial permissions.

**Upload the Software Package and Create a Trial Software Update Package**

To upload the software package and create a trial automatic software update package

1. Go to Admin > Software Updates > Automatic Software Updates.
2. Select the tab for the endpoint type of interest.
3. Click Upload Software Update.
4 In the **Upload Software Update** dialog box, verify the endpoint type and model.

5 If an activation key code is required to activate the software update, click the **Update Requires Key** check box and in the **Software Update Key File** field browse to the `.txt` key file received in “Request Update Activation Keys” on page 105.

The key is generated from the endpoint serial number and version number, and Polycom sends it as a text (.txt) file to the customer when new software is available. Customers can review their key history at [http://support.polycom.com](http://support.polycom.com).

6 In the **Software Update File** field, browse to the software update file you want to use.

7 Enter a meaningful description that will help other users to understand the purpose of the software update.

8 To trial the software with the group created previously, select **Trial Software** and from the **Select Trial Group** menu, select the trial group created in “Create a Local Trial Group” on page 114.

9 Click **OK**.

A trial automatic software update package for the endpoint type and model type appears in the **Automatic Software Update** list. You can tell it is a trial package, because the **Trial Group** column includes your entry.

The next time members of the trial group log into the system, their systems will be upgraded with the trial software package.

### Promote the Trial Software Update Package to Production

If you determine that the trial software update package is acceptable for production, you can then promote it to production.

**To promote a trial software update package to production**

1 Go to **Admin > Software Updates > Automatic Software Updates**.

2 Select the tab for product to update.

3 If areas are enabled, use the **Select Area** drop-down list to choose the area to which to promote the update.

   This drop-down list is only available if you manage more than one area.

4 Select the software update package of interest and click **Promote to Production**.

5 Click **Yes** to confirm the promotion.

   The package becomes a production automatic software update package.
Delete the Trial Software Update Package

If you determine that the trial software update package is unacceptable for production, you can delete it.

To delete a trial software update package

1. Go to Admin > Software Updates > Automatic Software Updates.
2. Select the tab for product to update.
3. Select the software update package of interest and click Delete Software Update.
4. Click Yes to confirm the deletion.
   The package is removed from the Automatic Software Updates list.
5. To return your trial group to the last production version of software, clear the Allow this version or newer option and click Update.
6. When all endpoints are back to the last production version of software, reset your automatic software update policy. See “Set an Automatic Software Update Policy” on page 107.

Automatic Software Updates for Peripherals

You can update the platform (operating system) and applications (if applicable) for peripherals connected to endpoints. Peripheral software updates can be in any of the following states:

- **Production** - The software update is configured for one or more groups that are using the software in production.
- **Trial** - The software update is configured for one or more groups that are trialing the software.
- **Both** - The software update is configured for one or more groups that are trialing the software and for one or groups are using the software in production.

For peripherals that permit software updates from the RealPresence Resource Manager system, you can download the updates from [http://support.polycom.com](http://support.polycom.com) and make them available from the RealPresence Resource Manager system web server. You also configure which updates are for trial or production use. The following topics describe software updates for peripherals:

- View Software Updates for Polycom Touch Controls
- Upload Peripheral Software Updates to the RealPresence Resource Manager System
- Configure Peripheral Updates for Production
• Configure Peripheral Updates for Trial

**View Software Updates for Polycom Touch Controls**

To view software updates for peripherals

1. Go to Admin > Software Updates > Automatic Software Updates.
2. Select the Touch Control tab.

   The tab includes this information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Area</td>
<td>Allows you to specify an area to which to apply the update.</td>
</tr>
<tr>
<td>Production URL</td>
<td>URL where the peripheral can access software updates configured for production use. The URL consists of the IP dress of the RealPresence Resource Manager system plus /repo.</td>
</tr>
<tr>
<td>Trial URL</td>
<td>URL where the peripheral can access software updates configured for trial use. The URL consists of the IP dress of the RealPresence Resource Manager system plus /repotrial.</td>
</tr>
<tr>
<td>Package Name</td>
<td>Displays the name of the software update package. Updates listed as platform are updates to the peripheral’s operating system. Other updates are for specific applications.</td>
</tr>
<tr>
<td>Description</td>
<td>The meaningful name given to the software update package when it was created</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the software package</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the software update. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None - The software update has not been configured for production or trial.</td>
</tr>
<tr>
<td></td>
<td>• Production - The software update is configured for production. It is available only from the Production URL.</td>
</tr>
<tr>
<td></td>
<td>• Trial - The software update is configured for trial. It is available only from the Trial URL.</td>
</tr>
<tr>
<td></td>
<td>• Both - The software update is configured for both production and trial. It is available from both the Production URL and the Trial URL.</td>
</tr>
<tr>
<td>Uploaded</td>
<td>The date and time when the software update package was uploaded</td>
</tr>
</tbody>
</table>
Upload Peripheral Software Updates to the RealPresence Resource Manager System

After you download the software updates from http://support.polycom.com and save them on your hard drive, you can upload them to the RealPresence Resource Manager system web server.

**To upload software updates to the RealPresence Resource Manager system**

1. Go to Admin > Software Updates > Automatic Software Updates.
2. Select the tab for the peripheral.
3. Click Upload Software Update.
4. In the Select File to Upload dialog box, navigate to and select the software update that you saved to your hard drive.
5. Click Open.

The update is added to the list on the peripheral tab.

---

If this is the first update for the platform or an application, the update is automatically configured for production.

---

Configure Peripheral Updates for Production

**To configure software updates for production**

1. Go to Admin > Software Updates > Automatic Software Updates.
2. Select the tab for the peripheral.
3. Click Configure Production.

The Configure Production dialog box includes the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Platform</td>
<td></td>
</tr>
<tr>
<td>Platform Description</td>
<td>The meaningful name given to the platform software update package when it was created</td>
</tr>
</tbody>
</table>
From the Configure Platform section, select the platform version to configure for production.

You can select only one platform version for production.

5 Click Configure Application.

6 For each application, select the version to configure for production from the Platform Compatible drop-down list.

The version selected must be compatible with the platform version listed in the column heading. If the application is not selected (no check mark), the application will not be configured for production.
Click OK.

From the peripheral itself, the configured software updates are now available using the Production URL.

**Configure Peripheral Updates for Trial**

To configure software updates for trial

1. Go to Admin > Software Updates > Automatic Software Updates.
2. Select the tab for the peripheral.
3. Click Configure Trial.

The Configure Trial dialog box includes the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Platform</strong></td>
<td></td>
</tr>
<tr>
<td>Platform Description</td>
<td>The meaningful name given to the platform software update package when it was created</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the platform software update. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None - The software update has not been configured as production or trial.</td>
</tr>
<tr>
<td></td>
<td>• Production - The software update is configured as production. It is available only from the Production URL.</td>
</tr>
<tr>
<td></td>
<td>• Trial - The software update is configured as trial. It is available only from the Trial URL.</td>
</tr>
<tr>
<td></td>
<td>• Both - The software update is configured as both production and trial. It is available from both the Production URL and the Trial URL.</td>
</tr>
<tr>
<td><strong>Configure Application</strong></td>
<td></td>
</tr>
<tr>
<td>Application Description</td>
<td>The meaningful name given to the application software update package when it was created</td>
</tr>
<tr>
<td>Platform Compatible</td>
<td>Column title shows the version of the currently selected platform. Use the drop-down list to select available application versions that match the platform version.</td>
</tr>
</tbody>
</table>
From the **Configure Platform** section, select the platform version to configure for trial.

You can select only one platform version for trial.

**5** Click **Configure Application**.

**6** For each application, select the version to configure for trial from the **Platform Compatible** drop-down list.

The version selected must be compatible with the platform version listed in the column heading. If the application is not selected (no check mark), the application will not be configured for trial.

**7** Click **OK**.

From the peripheral itself, the configured software updates are now available using the **Trial URL**.

---

### Using Scheduled Software Updates

The scheduled software update feature is enabled at the RealPresence Resource Manager system. An administrator with **System Setup** permissions can schedule software updates for one endpoint or a group of endpoints to occur immediately or for a date and time in the future.

Some notes about scheduled software updates:

- **Until the RealPresence Resource Manager system successfully updates an endpoint scheduled for updating, the update remains in the **Pending** or **In Progress** state and the RealPresence Resource Manager system attempts to update the endpoint until it succeeds or until the update is cancelled.**

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Status     | The current status of the application software update. Possible values are:  
  - **None** - The software update has not been configured as production or trial.  
  - **Production** - The software update is configured as production. It is available only from the **Production URL**.  
  - **Trial** - The software update is configured as trial. It is available only from the **Trial URL**.  
  - **Both** - The software update is configured as both production and trial. It is available from both the **Production URL** and the **Trial URL**. |
If an endpoint scheduled for update is **In a Call**, the RealPresence Resource Manager system waits until the call ends before updating the endpoint. The system checks the endpoint at 15 minute intervals.

If an endpoint scheduled for update is **Offline**, the RealPresence Resource Manager system attempts to connect to the endpoint every hour until the endpoint is **Online**.

A software update may reboot the endpoint.

This section includes these topics:

- “Supported Endpoints for Scheduled Software Updates” on page 122
- “Schedule the Software Update for Endpoints” on page 122
- “Scheduled Software Update View” on page 123
- “View Scheduled Software Update Information” on page 125
- “View List of Software Update Packages” on page 125

## Supported Endpoints for Scheduled Software Updates

Scheduled software updates are available for these endpoint types.

- HDX Series—when operating in standard management mode
- LifeSize
- TANDBERG T150
- TANDBERG C-Series
- TANDBERG MXP series

## Schedule the Software Update for Endpoints

Only users with the administrator role can schedule software updates. Users with the area administrator role cannot schedule software updates.

**To schedule one or more endpoints for software update**

1. Go to **Endpoint > Scheduled Software Update**.
2. As needed, use the **Filter** to customize the endpoint list.
3. Select the endpoints of interest and click **Software Update**.
4. In the **Schedule Software Update** dialog box, specify when the update should occur.
   a. In the **Schedule** field, select **Now** or **Later**.
   b. If you select **Later**, enter a **Date** and **Time** for the update.
Select either **Use Server Date/Time** or **Use Endpoint Date/Time** as these may differ.

5 Select from these options.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove address book entries</td>
<td>Select this check box to have all local address book entries removed after the update.</td>
</tr>
<tr>
<td>Remove system files</td>
<td>Select this check box to have all endpoint settings removed after the update. You must then reconfigure the endpoint.</td>
</tr>
<tr>
<td>Allow endpoint to be a DHCP server</td>
<td></td>
</tr>
</tbody>
</table>

You may apply a single software update request to multiple endpoint models. If the request includes one or more scheduling options that are not valid for a selected endpoint model, the system applies only the options that are valid.

6 Click **Schedule**.

For each endpoint selected, the status changes to **Pending** and the date and time for the software update appears in the **Scheduled** column.

**Scheduled Software Update View**

Use the **Scheduled Software Update View**, available from the **Endpoint** menu, to:

- View the list of endpoints that are eligible for a scheduled software update
- Schedule one or more endpoints for a software update
- Cancel a software update.

**Endpoint List in the Scheduled Software Update View**

By default the **Endpoint** list in the **Scheduled Software Update View** displays all endpoints eligible for scheduled software update.

The **Endpoint** list in the **Scheduled Software Update View** has the following information.
Scheduled Software Update View Actions

Besides providing access to the endpoint views, the **Action** section for the **Scheduled Software Update View** will also include these actions:
### Action

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Update</td>
<td>Schedule software update for the selected endpoints.</td>
</tr>
<tr>
<td>Cancel Update</td>
<td>Cancel a scheduled or in progress software update operation.</td>
</tr>
<tr>
<td>Clear Status</td>
<td>Change the status column for an endpoint to the <strong>Clear</strong> state.</td>
</tr>
</tbody>
</table>

For information about these endpoint actions, see “Updating Endpoint and Peripheral Software” on page 101.

---

### View Scheduled Software Update Information

**To view information about software updates that are scheduled or for endpoints that are eligible for scheduled software updates**

1. Go to **Endpoint > Scheduled Software Update**.
2. As needed, use the **Filter** to customize the endpoint list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, and **Site**.
3. Select the endpoint of interest.
4. In the **Endpoint Summary** pane, expand the **Software Update Details** tab. For more information, see “Software Update Details” on page 220.

---

### View List of Software Update Packages

**To view the list of scheduled software update packages**

>> Go to **Admin > Software Updates > Scheduled Software Updates**.

The **Scheduled Software Updates** page appears listing all of the endpoint types and models for which the RealPresence Resource Manager system can perform a scheduled software update. It includes this information. If a software update package has been uploaded to the system, the Description and Uploaded fields are populated for the endpoint.

---

### Cancel Software Updates

You can cancel scheduled software updates for an endpoint. You cannot explicitly cancel automatic software updates for an endpoint. You must do that at the endpoint.
To cancel scheduled software updates

1. Go to Endpoint > Scheduled Software Update.
2. As needed, use the Filter to customize the endpoint list.
3. Select the endpoint or endpoints of interest and click Cancel Update.
   A confirmation dialog box appears. The dialog box may indicate that one or more of the selected endpoints had a software update in progress.
4. Click Ok to cancel in progress and future software updates for the selected endpoints and clear their status.
   You can cancel software update operations that are in progress, but you may wish to check the endpoint afterward to verify it was left in an operational state.
Provisioning Endpoints

The Polycom® RealPresence® Resource Manager system can provision several types of endpoints. Endpoint provisioning, which requires provisioning profiles, allows an administrator to remotely configure multiple endpoints of the same type with a standard set of settings. This eliminates the need to configure each endpoint individually either through the hand-held remote or the endpoint’s web interface.

The RealPresence Resource Manager system supports three types of endpoint provisioning: bundled, automatic, and scheduled. Enable endpoints for only one type of provisioning.

This chapter describes RealPresence Resource Manager system endpoint provisioning operations. It includes these topics:

- “Provisioning Best Practices” on page 127
- “Provisioning in a Multi-Tenancy Environment” on page 128

Provisioning Best Practices

To use the available provisioning options most effectively, we recommend the following:

1. For each site in the RealPresence Resource Manager system, configure the site provisioning details as needed for each site. See “Add a Site” on page 479.

2. On each HDX model, configure the HDX system settings that are available in bundled provisioning for that model. Then download the provisioning bundle for each HDX model to the RealPresence Resource Manager system. See “Bundled Provisioning of Endpoints” on page 139.

3. If you need unique provisioning settings for one or more groups of users, create automatic provisioning profiles with those settings and apply them to the appropriate groups. See “Automatic Provisioning of Endpoints” on page 131 and “Add a Local Group” on page 289.

For example, you may want to set a higher bit rate for the executives of your organization or for conference rooms used for large video
conferences. You can create a group for these users/rooms and give that group an automatic provisioning profile with a higher bit rate.

Provisioning Profile Order and Priority

Automatic provisioning profiles are associated with groups, but what about those users who belong to more than one group—what determines their experience? When you add new profiles, you assign a **Profile Order**. The **Profile Order** determines which provisioning profile takes priority.

Consider the following example:

- Jason Smith is part of the Support group and also part of the Executive group.
- The Support group is assigned an automatic provisioning profile named Low-Bandwidth, which allows a maximum speed for receiving calls of 128kbps.
- The Executive group is assigned an automatic provisioning profile called High-Bandwidth, which allows a maximum speed for receiving calls of 1920kbps.
- The Low-Bandwidth profile is assigned a profile order of 1, while the High-Bandwidth profile is assigned a profile order of 2.

In this example, Jason’s endpoint is provisioned with the Low-Bandwidth provisioning profile, because it has the higher priority.

So when you add provisioning profiles, you may want to assign provisioning profiles with more robust privileges a higher priority than those providing less privileges.

Order of Provisioning Operations

Provisioning information is applied in the following order:

1. Bundled provisioning, if a bundle exists for the same model.
2. Automatic provisioning profile, if the endpoint is part of a group assigned a profile.
3. Site provisioning, which takes precedence.

For information about how to download a provisioning profile, see “Bundled Provisioning of Endpoints” on page 139.

Provisioning in a Multi-Tenancy Environment

Polycom recommends using automatic provisioning in a multi-tenancy environment where some endpoints may reside outside the firewall.
Automatic provisioning is client-to-server over HTTPS which makes it more secure and firewall-friendly.

For more information, see the following:

- “Standard versus Dynamic Management” on page 75
- “Automatic Provisioning of Endpoints” on page 131
Automatic Provisioning of Endpoints

The Polycom® RealPresence® Resource Manager system can provision several types of endpoints. Endpoint provisioning, which requires provisioning profiles, allows an administrator to remotely configure multiple endpoints of the same type with a standard set of settings. This eliminates the need to configure each endpoint individually either through the hand-held remote or the endpoint’s web interface.

The RealPresence Resource Manager system supports three types of endpoint provisioning: bundled, automatic, and scheduled. Enable endpoints for only one type of provisioning.

This chapter describes RealPresence Resource Manager system endpoint provisioning operations. It includes these topics:

- “Automatic Provisioning” on page 131
- “Using Automatic Provisioning” on page 132

Automatic Provisioning

In dynamic management mode, when an endpoint starts up and at designated intervals thereafter, it automatically polls for new provisioning information from the RealPresence Resource Manager system. The provisioning information is sent in XML format over a secure HTTPS connection.

Endpoints do not poll for provisioning information if they are in a call. They restart polling after the call ends.

The RealPresence Resource Manager system manages video and audio endpoints. However, the system also manages users, because endpoints are only useful when they provide access to users.

Automatic provisioning, which controls the automatic configuration of dynamically managed endpoints and the management of its video resources, is also tied to users and groups. That’s because some users and groups may require significantly more video resources than others.
Currently, automatic provisioning is available for:

- Polycom VVX systems deployed in dynamic management mode
- Polycom HDX systems deployed in dynamic management mode
- Polycom CMA Desktop clients
- RealPresence Mobile clients

Polycom CMA Desktop provisioning occurs on a session by session basis.

**Default Automatic Provisioning Profiles**

Automatic provisioning is enabled at the endpoint, but the RealPresence Resource Manager system must have automatic provisioning profiles for both the endpoint and the site at which the endpoint resides. So to ensure out-of-box usability, the RealPresence Resource Manager system comes with Default Provisioning Profiles for both. However, you can edit these default profiles to meet your needs or add additional provisioning profiles to assign different video resources to different groups of users.

- If an automatic provisioning profile provisions a setting that the endpoint is not capable of fulfilling, the endpoint will ignore those settings.
- The name of the Default Provisioning Profile is stored in the system database and is not localized into other languages. If you wish to localized it into your language, edit the profile and give it a new profile name.

For information about how to add an automatic provisioning profile, see “Add an Automatic Provisioning Profile” on page 134.

**Using Automatic Provisioning**

This topic describes the automatic provisioning operations a user assigned the Device Administrator role can perform. These are:

- “Automatic Provisioning View” on page 133
- “View the Automatic Provisioning List and Details” on page 134
- “Add an Automatic Provisioning Profile” on page 134
Automatic Provisioning View

Use the Endpoint > Automatic Provisioning menu to see the list of endpoints that are registered to the system for automatic provisioning.

Endpoint List in the Automatic Provisioning View

By default the endpoint list in the Automatic Provisioning View displays the list of Polycom HDX system endpoints registered to the RealPresence Resource Manager system for automatic provisioning.

The endpoint list in the Automatic Provisioning View has the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Filter | The filter choice for endpoint types that can be automatically provisioned. Possible values include:  
  - All—Displays all dynamically managed endpoint systems registered to the system.  
  - HDX Series—Displays just the Polycom HDX systems registered to the system and deployed in dynamic management mode.  
  - CMA Desktop—Displays just the Polycom CMA Desktop systems registered to the system.  
  - VVX—Displays just the Polycom VVX systems registered to the system.  
  - RealPresence Mobile—Displays just the RealPresence Mobile systems registered to the system. |
| Status | The status of the endpoint's last provisioning process. Possible values include:  
  - Success  
  - Failed  
  - Clear |
| Name | The assigned name of the endpoint. |

Note

The system assigns Polycom CMA Desktop systems a user name of LastName_Firstname_CMADesktop.
Actions in the Automatic Provisioning View

Because automatic provisioning is managed by the endpoint, there are no context-sensitive commands available in the Automatic Provisioning View.

View the Automatic Provisioning List and Details

Users with the Device Administrator, Administrator or the Area Administrator role can view details about automatic provisioning.

To view the automatic provisioning list and details about an automatic provisioning operation

1. Go to Endpoint > Automatic Provisioning.
2. As needed, use the Filter to customize the Endpoint list.
3. Select the endpoint of interest.
4. Expand the Provisioning Details tab in the right pane.

Add an Automatic Provisioning Profile

This topic describes how to add automatic provisioning profiles.

Add provisioning profiles in the middle of the work day, not first thing in the morning.
When you add an automatic provisioning profile, the RealPresence Resource Manager system immediately rolls it out. If it rolls it out first thing in the morning, people who need to attend a “start the day” conference will have to first wait for their endpoint to be provisioned. Polycom recommends implementing profiles in the middle of the work day and then let the provisioning occur at the designated polling interval.

Only users with the administrator role can add a provisioning profile.

**To add an automatic provisioning profile**

1. Go to Admin > Provisioning Profiles > Automatic Provisioning Profiles.
2. In the Automatic Provisioning Profiles page, click Add.
3. In the Add Profile dialog box, enter a name for the profile and click Next.
4. Complete the Settings sections of the Provisioning Fields dialog box.
   
   For a detailed description of the endpoint fields you can configure when adding a new automatic provisioning profile, see “Endpoint Fields for Automatic Provisioning” on page 193. You may find more implementation details about these fields in the endpoint system documentation.
5. Click OK.
   
   The provisioning profile appears at the bottom Automatic Provisioning Profiles list.
6. To change the priority order of the automatic provisioning profiles:
   
   a. Click in the Profile Order text box preceding the provisioning profile of interest and enter the priority for the profile.
   
   b. Click Update Profile Order.
      
      The system assigns the provisioning profile the selected priority and shuffles and reassigns priorities to the other provisioning profiles.

**Edit an Automatic Provisioning Profile**

**To edit an automatic provisioning profile**

1. Go to Admin > Provisioning Profiles > Automatic Provisioning Profiles.
2. In the Automatic Provisioning Profiles page, select the profile of interest and click Edit.
3 Edit the System Settings, Home Screen Settings, H.323 Settings, Call Settings, Audio Settings, and (if applicable) CMA Desktop Settings sections of the Provisioning Fields dialog box.

For a detailed description of the endpoint fields you can configure when adding a new automatic provisioning profile, see “Endpoint Fields for Automatic Provisioning” on page 193. You may find more implementation details about these fields in the endpoint system documentation.

4 Click OK.

The provisioning profile is updated.

**Edit the Profile Order for an Automatic Provisioning Profile**

**To edit the profile order for an automatic provisioning profile**

1 Go to Admin > Provisioning Profiles > Automatic Provisioning Profiles.

2 In the Automatic Provisioning Profiles page, select the profile of interest, click in the Profile Order text box preceding the provisioning profile of interest, and enter the priority for the profile.

3 Click Update Profile Order.

The system assigns the provisioning profile the selected priority and shuffles and reassigns priorities to the other provisioning profiles.

**Clone an Automatic Provisioning Profile**

**To clone an automatic provisioning profile**

1 Go to Admin > Provisioning Profiles > Automatic Provisioning Profiles.

2 In the Automatic Provisioning Profiles page, select the profile of interest and click Clone.

3 In the Clone Profile dialog box, enter a name for the new profile and click Save.

The provisioning profile appears last in the Automatic Provisioning Profiles list.

4 As needed, edit the profile.

See “Edit an Automatic Provisioning Profile” on page 135.
Delete an Automatic Provisioning Profile

To delete an automatic provisioning profile

1. Go to Admin > Provisioning Profiles > Automatic Provisioning Profiles.

2. In the Automatic Provisioning Profiles page, select the profile of interest and click Delete.

3. Click Yes to confirm the deletion.

   The profile is deleted from the system.
The Polycom® RealPresence® Resource Manager system supports a Bundled Provisioning model for dynamically managed HDX systems. With Bundled Provisioning, a RealPresence Resource Manager system administrator can download a provisioning bundle from any already configured HDX system. Any dynamically managed HDX system of the same model will receive the provisioning bundle when it next polls the RealPresence Resource Manager system for new provisioning information.

Some configuration settings on dynamically managed endpoints that the RealPresence Resource Manager system provisions are associated with the site where the endpoint system is located. Site provisioning takes precedence.

Bundled provisioning provides businesses with an efficient and effective way to provision HDX systems consistently across each model. HDX system users with administrative rights can still change the settings on an HDX system after the provisioning bundle is applied. However, if a newer bundle is sent by the RealPresence Resource Manager system, it will overwrite the user’s changes.

In this release, the HDX system parameters that may be provisioned in a bundle are limited to the following types:

- Camera configuration settings
- Monitor configuration settings
- Microphone configuration settings
- Security settings
- Home screen settings

This chapter describes RealPresence Resource Manager system bundled provisioning operations. It includes these topics:

- “How Bundled Provisioning Works” on page 140
- “View the Provisioning Bundle List” on page 140
- “Download a Provisioning Bundle” on page 141
- “Delete a Provisioning Bundle” on page 141
How Bundled Provisioning Works

In dynamic management mode, when an HDX system starts up and at designated intervals thereafter, it automatically polls for new provisioning information from the RealPresence Resource Manager system. If a provisioning bundle exists on the RealPresence Resource Manager system that matches the model of the polling HDX system, the provisioning bundle is sent over a secure HTTPS connection.

Endpoints do not poll for provisioning information if they are in a call. They restart polling after the call ends.

Provisioning information is applied in the following order:

1. Bundled provisioning, if a bundle exists for the same model.
2. Automatic provisioning profile, if the endpoint is part of a group assigned a profile.
3. Site provisioning, which takes precedence.

For information about how to download a provisioning profile, see “Download a Provisioning Bundle” on page 141.

This section describes the bundled provisioning operations a user assigned the Device Administrator or Area Administrator role can perform. These are:

- View the Provisioning Bundle List
- Download a Provisioning Bundle
- Delete a Provisioning Bundle

View the Provisioning Bundle List

To view the provisioning bundle list

1. Go to Endpoint > Bundled Provisioning.
2. As needed, use the Filter to customize the list of provisioning bundles.
Download a Provisioning Bundle

After you download a provisioning bundle for a specific HDX model, any dynamically managed HDX system of the same model will receive the provisioning bundle when the HDX system next polls the RealPresence Resource Manager system for new provisioning information.

If a provisioning bundle already exists for the model you select, the existing bundle is overwritten with the new one.

For more information about provisioning bundles, see “How Bundled Provisioning Works” on page 140.

To download a provisioning bundle

1. Go to Endpoint > Bundled Provisioning.
2. Click Download.
   The Download Provisioning Bundle From an Endpoint dialog lists all of the HDX systems registered with the system.
3. As needed, use the Filter to customize the endpoint list.
4. Select the HDX system that is configured the way you want for the provisioning bundle.
5. Complete the Bundle Name and Description fields.
6. Click Download.
   The system confirms that the bundle downloaded successfully.
7. Click OK.

Delete a Provisioning Bundle

When you no longer need a provisioning bundle for an HDX model, you can delete it. An existing provisioning bundle is also removed when you download a bundle for the same HDX model. The newly downloaded bundle overwrites the existing one.

1. Go to Endpoint > Bundled Provisioning.
2. As needed, use the Filter to customize the list of provisioning bundles.
3. Select the bundle you want to delete.
4. Click Delete.
5. Click Yes to confirm the deletion.
   The system confirms that the bundle was deleted.
Bundled Provisioning View

Use the Bundled Provisioning View to see the list of provisioning bundles available to dynamically managed HDX systems.

Endpoint List in the Bundled Provisioning View

By default the Bundled Provisioning View displays the list of provisioning bundles available for use by dynamically managed HDX systems.

The bundle list in the Bundled Provisioning View has the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>The filter choices for provisioning bundles that have been downloaded to the system. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Name—Filters by the name of the provisioning bundle.</td>
</tr>
<tr>
<td></td>
<td>• Model—Filters by the endpoint model.</td>
</tr>
<tr>
<td></td>
<td>• Creation Date—Filters by the date the provisioning bundle was downloaded and created on the system.</td>
</tr>
<tr>
<td></td>
<td>• Description—Filters by the description of the provisioning bundle.</td>
</tr>
<tr>
<td>Name</td>
<td>The name assigned to the provisioning bundle when it was downloaded and created on the system.</td>
</tr>
<tr>
<td>Model</td>
<td>The exact model of endpoint to which the provisioning bundle applies as defined when it was downloaded and created on the system.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>The date the provisioning bundle was downloaded and created on the system.</td>
</tr>
<tr>
<td>Description</td>
<td>The description assigned to the provisioning bundle when it was downloaded and created on the system.</td>
</tr>
</tbody>
</table>

Actions in the Bundled Provisioning View

The Actions section of the Bundled Provisioning View may include these context-sensitive commands.

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download</td>
<td>Create a new provisioning bundle by downloading the bundled from an HDX system on the network.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the selected bundled from the bundle list.</td>
</tr>
</tbody>
</table>
Scheduled Provisioning of Endpoints

Scheduled provisioning is enabled at the Polycom® RealPresence® Resource Manager system. To schedule an endpoint for provisioning, the RealPresence Resource Manager system must already have a scheduled provisioning profile created for the endpoint.

This chapter describes RealPresence Resource Manager system endpoint provisioning operations. It includes these topics:

- “How Scheduled Provisioning Works” on page 143
- “Scheduled Provisioning Profiles” on page 144
- “Scheduled Provisioning Notes” on page 144
- “Using Scheduled Provisioning” on page 145

How Scheduled Provisioning Works

Users with the Device Administrator or Area Administrator role can schedule provisioning for one endpoint or a group of endpoints; and they can schedule provisioning to occur immediately or for a date and time in the future. The provisioning data is sent in XML format over a secure HTTPS connection.

Scheduled provisioning is available for these endpoint types:

- VSX Series endpoints
- Selected TANDBERG endpoints—TANDBERG 150, 990, 880, and 770 endpoints
- HDX Series—Polycom HDX systems deployed in standard management mode
Scheduled Provisioning Profiles

The RealPresence Resource Manager system does not include a default profile for scheduled provisioning. You must create a profile before you can schedule an endpoint for provisioning. Create a different profile for each endpoint type (Polycom HDX system or Polycom CMA Desktop) and group of users.

Some examples of when to use scheduled provisioning profiles follow.

- To apply a standard set of options to each new endpoint
  By creating templates of standard settings for different types of endpoints, or for the needs of different users, you can have the RealPresence Resource Manager system apply all the settings at once. After the endpoint is connected and registered with the RealPresence Resource Manager system, you can use a provisioning profile that defines a range of other options.

- To update the password for all endpoints of a particular type
  For security purposes, you can create a provisioning profile to update the password for endpoints on a regular basis and reuse the same profile quarterly. You might have several profiles, one for each type of endpoint to update.

For information about how to add a scheduled provisioning profile, see “Add a Scheduled Provisioning Profile” on page 146.

For a detailed description of the endpoint fields you can configure when adding a new automatic provisioning profile, see “Endpoint Fields for Automatic Provisioning” on page 193. You may find more implementation details about these fields in the endpoint system documentation.

The sections may differ depending on the endpoint type selected.

Scheduled Provisioning Notes

Some notes about scheduled provisioning profiles and the scheduled provisioning of endpoints:

- Each page in the scheduled Provisioning Fields dialog box has a Provision This Page option. When this option is selected, the system provisions all of the values on that page. When this option is not selected, the system does not provision any of the values on that page. At least one page must be provisioned, or the system returns an error stating, “No data to save in profile. Either press Cancel or add pages.”

- Until the RealPresence Resource Manager system successfully provisions an endpoint scheduled for provisioning, provisioning remains in the Pending state and the system attempts to provision the endpoint until it succeeds or until the provisioning is cancelled.
• If an endpoint scheduled for provisioning is **In a Call**, the system waits until the call ends before provisioning the endpoint. The system checks the endpoint at 15 minute intervals.

• If an endpoint scheduled for provisioning is **Offline**, the system attempts to connect to it at 60 minute intervals until the endpoint is **Online**.

• Provisioning may reboot the endpoint.

• You can schedule provisioning for an unlimited number of endpoints, but the system may limit the number of active provisioning processes.

---

**Using Scheduled Provisioning**

This section describes the scheduled provisioning tasks a user assigned the Device Administrator or Area Administrator role can perform. These are:

- “**View the Scheduled Provisioning List and Details**” on page 145
- “**Add a Scheduled Provisioning Profile**” on page 146
- “**Edit a Scheduled Provisioning Profile**” on page 146
- “**Clone a Scheduled Provisioning Profile**” on page 147
- “**Delete a Scheduled Provisioning Profile**” on page 147
- “**Schedule an Endpoint for Provisioning**” on page 148
- “**Check the Status of a Scheduled Provisioning**” on page 148
- “**Clear the Status of Scheduled Provisioning**” on page 149
- “**Cancel a Scheduled Provisioning**” on page 149

---

**View the Scheduled Provisioning List and Details**

To view the automatic provisioning list and details about a scheduled provisioning operation

1. Go to **Endpoint > Scheduled Provisioning**.
2. As needed, use the **Filter** to customize the **Endpoint** list.
3. Select the endpoint of interest.
4. Expand the **Provisioning Details** tab in the **Device Details** section.
Add a Scheduled Provisioning Profile

To add a scheduled provisioning profile

1. Go to Admin > Provisioning Profiles > Scheduled Provisioning Profiles.
2. In the Scheduled Provisioning Profiles page, click Add.
3. In the Add Profile dialog box, select the Endpoint Type for the provisioning profile, enter a name for the profile, and click Next.
4. As needed, select Provision This Page and complete the General Settings, Video Network, Monitors, Cameras, Audio Settings, LAN Properties, and Global Services sections of the Provisioning Fields dialog box.

   For information about these fields, see “Endpoint Fields for Scheduled Provisioning” on page 196.

   The sections may differ depending on the endpoint type selected.
5. Click OK.

   The provisioning profile appears in the updated Scheduled Provisioning Profiles list.

Edit a Scheduled Provisioning Profile

To edit a scheduled provisioning profile

1. Go to Admin > Provisioning Profiles > Scheduled Provisioning Profiles.
2. In the Scheduled Provisioning Profiles list, select the profile of interest and click Edit Profile.
3. As needed, select Provision This Page and complete the General Settings, Video Network, Monitors, Cameras, Audio Settings, LAN Properties, and Global Services sections of the Provisioning Fields dialog box.

   For a detailed description of the endpoint fields you can configure when adding a new scheduled provisioning profile, see “Endpoint Fields for Scheduled Provisioning” on page 196.

   You may find more implementation details about these fields in the endpoint system documentation.

   The sections may differ depending on the endpoint type selected.
4. Click OK.

   The provisioning profile is updated.
Clone a Scheduled Provisioning Profile

To clone a scheduled provisioning profile

1. Go to Admin > Provisioning Profiles > Scheduled Provisioning Profiles.
2. In the Scheduled Provisioning Profiles page, select the profile of interest and click Clone Profile.
3. In the Clone Profile dialog box, enter a name for the new profile and click Save.

   The provisioning profile appears first in the updated Scheduled Provisioning Profiles list.
4. Edit the sections of the Provisioning Fields dialog box.

   For information about these fields, see “Endpoint Fields for Scheduled Provisioning” on page 196.

   The sections may differ depending on the endpoint type selected. For more information on these fields, see the product documentation for the selected endpoint.
5. Review each page of the scheduled provisioning profile and determine if you want the parameters on the page provisioned. If you do want the parameters on the page provisioned, select Provision This Page.
6. Click OK.

   The provisioning profile is updated.

Delete a Scheduled Provisioning Profile

To delete a scheduled provisioning profile

1. Go to Admin > Provisioning Profiles > Scheduled Provisioning Profiles.
2. In the Scheduled Provisioning Profiles page, select the profile of interest and click Delete Profile.
3. Click Yes to confirm the deletion.

   The profile is deleted from the RealPresence Resource Manager system.
Schedule an Endpoint for Provisioning

To schedule an endpoint for provisioning
1  Go to Endpoint > Scheduled Provisioning.
2  As needed, use the Filter to customize the endpoint list.
3  Select the endpoints of interest.
4  Click Provision.
5  In the Schedule Endpoint Provisioning dialog box, select the appropriate provisioning profile.
6  In the Schedule field, select Now or Later.
7  If you select Later, enter a Date and Time for the provisioning.
8  Select either Use Server Date/Time or Use Endpoint Date/Time as these may differ.
9  Click Schedule.
   The Scheduled Provisioning View reappears.
10 Click Refresh and check the Pending column for the provisioning status.
   For each endpoint you selected, the name of the profile appears in the Pending column, and the date and time you entered appears in the Scheduled column.

Check the Status of a Scheduled Provisioning

To check the status of a scheduled provisioning
1  Go to Endpoint > Scheduled Provisioning.
2  As needed, use the Filter to customize the endpoint list.
3  Select the endpoint of interest.
4  Expand the Provisioning Details tab in the Device Details section.
   For a detailed description of the endpoint fields you can configure when adding a new scheduled provisioning profile, see “Endpoint Fields for Scheduled Provisioning” on page 196. You may find more implementation details about these fields in the endpoint system documentation.
Scheduled Provisioning of Endpoints

Clear the Status of Scheduled Provisioning

To clear the status of a scheduled provisioning
1. Go to Endpoint > Scheduled Provisioning.
2. As needed, use the Filter to customize the endpoint list.
3. Select the endpoints of interest.
4. Click Clear Status.
   The endpoint provisioning status returns to Clear.

Cancel a Scheduled Provisioning

You can only cancel provisioning of a Pending process. You cannot cancel the provisioning of an endpoint while it is In Progress.

To cancel a pending scheduled provisioning
1. Go to Endpoint > Scheduled Provisioning.
2. As needed, use the Filter to customize the endpoint list.
3. Select the endpoints of interest.
4. Click Cancel Provision.
   The provisioning operation is cancelled and the provisioning status returns to Clear.

Scheduled Provisioning View

Use the Scheduled Provisioning View to:
• View the list of endpoints that are eligible for scheduled provisioning
• Schedule one or more endpoints for provisioning
• Cancel a scheduled provisioning

Endpoint List in the Scheduled Provisioning View

By default the endpoint list in the Scheduled Provisioning View displays the list of Polycom HDX system endpoints registered to the RealPresence Resource Manager system that are eligible for scheduled provisioning.

The Endpoint list in this view has the following information.
### Field | Description
--- | ---
Filter | The filter choice for endpoint types that can be scheduled for provisioning. Possible values include:
- **HDX Series**—Displays the Polycom HDX systems operating in standard management mode.
- **LifeSize®**
- **QDX Series**
- **TANDBERG T150**
- **TANDBERG C-Series**
- **TANDBERG MXP**
- **V and VSX Series**

Status | The status of the endpoint’s last provisioning process. Possible values include:
- **Success**
- **Pending**
- **Failed**
- **Clear**

Name | The system name of the endpoint.

Type | The type of endpoint. Scheduled provisioning is only available for the endpoints types listed in this table as **Filter** selections.

IP Address | The IP address assigned to the endpoint.

Last | The date and time of the endpoint’s last provisioning, unless its status has been cleared.

Pending | When the endpoint is scheduled for provisioning, this field shows the provisioning profile to be used for the scheduled provisioning process.

Scheduled | When the endpoint is scheduled for provisioning, this field shows the date and time for the next scheduled provisioning process.

### Actions in the Scheduled Provisioning View

Besides providing access to the endpoint views, the **Actions** section of the **Scheduled Provisioning View** also includes these commands:
Scheduled Provisioning of Endpoints

You can perform these operations on multiple endpoints at the same time. To select multiple endpoints, hold the control key while you select the endpoints.

For information about these endpoint actions, see “Scheduled Provisioning of Endpoints” on page 143.

<table>
<thead>
<tr>
<th>Action</th>
<th>Use this action to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision</td>
<td>Schedule provisioning for the selected endpoint(s).</td>
</tr>
<tr>
<td>Cancel Provision</td>
<td>Cancel a previously scheduled provisioning operation.</td>
</tr>
<tr>
<td>Clear Status</td>
<td>Change the status column for a endpoint to the Clear state.</td>
</tr>
</tbody>
</table>
Automatic Provisioning Endpoints for SIP Server Integration

The Polycom® RealPresence® Resource Manager system allows you to automatically provision endpoints with the integration with SIP servers by provisioning some Polycom endpoints with the SIP credentials and SIP settings they need.

SIP settings can only be provisioned using automatic provisioning. You cannot use scheduled or bundled provisioning to provision SIP settings. For more information about automatic provisioning, see “Automatic Provisioning of Endpoints” on page 131.

You can configure the RealPresence Resource Manager system to dynamically provision SIP settings for the following SIP servers:

- Standard (a SIP server that meets SIP standards)
- Microsoft Lync
- BroadSoft BroadWorks
- Polycom DMA system
- Siemens OpenScape
- Avaya Aura Session Manager
- Cisco Unified Communications Manager

This section includes the following topics:

- “SIP Provisioning Considerations” on page 153
- “Provision Endpoints with SIP Server Settings” on page 154

SIP Provisioning Considerations

- You can only provision SIP settings when you use automatic provisioning.
- SIP settings are configured at the site level.
• If the SIP server uses a different authentication directory than your RealPresence Resource Manager system and requires unique authentication for each endpoint, you need to import both user information and SIP URLs before provisioning SIP settings.

• Provisioning Microsoft SIP requires additional steps, see “Provision Group for Microsoft Lync or Microsoft Office Communications Server Integration” on page 158.

SIP Server Authentication Requirements

You must understand your SIP server’s authentication requirements when you provision SIP settings for endpoints managed by the RealPresence Resource Manager system.

SIP server authentication requirements differ according to your environment.

• If your SIP server does not require credentials, you do not need to indicate any credentials to use when provisioning.

• If your SIP server requires a common username and password for all endpoints registering to the SIP server, you need to explicitly provision that username and password to applicable endpoints.

• If your SIP server uses the same authentication database (i.e., Microsoft Active Directory) as the RealPresence Resource Manager system, you need to use the RealPresence Resource Manager system provisioning credentials.

• If your SIP server does NOT use the same authentication database as the RealPresence Resource Manager system and requires unique usernames and passwords for each endpoint, you need to import the usernames from the SIP server and import SIPURI information for the associated endpoints before you can use automatic provisioning. You can then use the RealPresence Resource Manager system provisioning credentials to provision endpoints.

Provision Endpoints with SIP Server Settings

The RealPresence Resource Manager system supports the integration with various SIP servers by provisioning endpoints SIP settings they need.

After you provision endpoints with SIP settings, all endpoints receive directory information from one of those servers. You are no longer using the enterprise directory or the other directory functions in the RealPresence Resource Manager system.

The RealPresence Resource Manager system supports SIP to establish conference connections. If you want to use SIP, you must enable it and configure SIP settings. You must also upload SIP URI data.
To provision endpoints with the information required to integrate with these SIP servers, you must complete the following tasks:

- “Creating Authentication Information for SIP Endpoints” on page 155
- “Import SIP URI Data” on page 155
- “Provision SIP Settings for SIP Server Integration” on page 156

Creating Authentication Information for SIP Endpoints

To have the RealPresence Resource Manager system automatically provision a Polycom endpoint for SIP integration, the endpoint must use the same credentials (username and password) to access both the SIP server and the RealPresence Resource Manager system. Only then can the RealPresence Resource Manager system automatically provision SIP settings.

If the SIP server uses a third-party database for authentication that the RealPresence Resource Manager system is not aware of, you need to import both the user information and SIP URI information from the SIP server.

1. Create a RealPresence Resource Manager system local user account for the endpoint that matches the username and password. To save time, you can import the users that you need, see “Import Users” on page 284.

2. Associate those users with endpoints, see “Associate a User with an Endpoint” on page 98.

3. Import SIP URI data for those users, see “Import SIP URI Data” on page 155

Import SIP URI Data

After you enable and configure SIP, you must import your endpoint SIP URI information from your SIP server. The SIP URI is used as the endpoint’s address.

If you are using Microsoft as your SIP server, you do not need to import SIP URI data. The RealPresence Resource Manager system can retrieve the SIP URI from the enterprise directory.

1. Create a CSV file in the format described here. The import requires a CSV file in the following format:

   domain,username,deviceType,URI

   where:

   - domain—Specifies the domain the user uses to log in to the RealPresence Resource Manager system.
— **username**—Specifies the RealPresence RealPresenceResource Manager system user name.

— **deviceType**—Specifies the device type (valid values are HDX, VVX, and CMADesktop or RPMobile).

— **URI**—Specifies the SIP URI for this user.

  For example: local, johndoe, HDX, johndoe@example.com

2. From the RealPresence Resource Manager system, go to **Admin > Uploads**.

   a. Click **Upload**.

   b. Navigate to the CSV file, select it, and click **Open**.

Whenever you add new users or rooms or need change a SIP URI, you must provide SIP URI data. For the methods available for editing the SIP URI, see “Edit SIP URI Data” on page 156.

**Edit SIP URI Data**

You can edit SIP URI data in the following ways:

- Upload a CSV file that has changes or new data. Data in the CSV file is added to any existing data. For information about the CSV file format and the upload process, see “Import SIP URI Data” on page 155.

- Edit individual users or rooms. For each RealPresence Resource Manager system user or room, you can add or edit the SIP URI in the **Dial String Reservations** section of the **Edit User** or **Edit Room** dialog box.

**Provision SIP Settings for SIP Server Integration**

By default, SIP is disabled in site provisioning. This procedure describes how to change existing site provisioning settings so that they provision integration with a SIP server.

When you add a site to the RealPresence Resource Manager system, you also set up site provisioning, which includes the SIP settings. Be sure to enable SIP and configure the servers, protocol, and credentials needed for your SIP server.

**To provision SIP for integration with a SIP server**

1. Go to **Admin > Topology > Sites**.

2. In the **Sites** page, select the site of interest and click **Edit Site Provisioning Details**.

3. In the **Edit Site Provisioning Details** dialog box, click **SIP Settings** and select these options.
### Fields Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Specify whether to enable SIP calls.</td>
</tr>
<tr>
<td>Automatically Discover SIP Servers</td>
<td>The RealPresence Resource Manager system will issue a DNS query to locate the SIP server and provision that information to endpoints.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Specify the IP address or DNS name of the SIP proxy server for the network.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Specify the IP address or DNS name of the SIP registrar server for the network.</td>
</tr>
<tr>
<td>- In an Microsoft Office Communications Server 2007 or Microsoft Lync Server 2010 environment, specify the IP address or DNS name of the Office Communications Server or Lync Server server.</td>
<td></td>
</tr>
<tr>
<td>- If registering a remote HDX system with an Office Communications Server Edge Server or Lync Server Edge Server, use the fully qualified domain name of the access edge server role.</td>
<td></td>
</tr>
<tr>
<td>Backup Registrar Server</td>
<td>Specify the IP address or DNS name of a backup SIP registrar server for the network</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure determines which protocol is required.</td>
</tr>
<tr>
<td>- Auto enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments.</td>
<td></td>
</tr>
<tr>
<td>- TCP provides reliable transport via TCP for SIP signaling.</td>
<td></td>
</tr>
<tr>
<td>- UDP provides best-effort transport via UDP for SIP signaling.</td>
<td></td>
</tr>
<tr>
<td>- TLS provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060.</td>
<td></td>
</tr>
</tbody>
</table>
You must set up the Microsoft Lync or Office Communications Server group that needs to be provisioned to endpoints in each automatic provisioning profile. This controls the directory that endpoints can see.

- You cannot provision integration with a Microsoft Lync or Office Communications Server via scheduled provisioning.
- If the endpoint being provisioned is not capable of integration with a Microsoft Lync or Office Communications Server, the endpoint will ignore this settings.
- The group setting here applies to both Microsoft Lync and Office Communication Server.
To provision integration with Microsoft Lync or Office Communications Server

1 Go to Admin > Provisioning Profiles > Automatic Provisioning Profiles.

2 In the Automatic Provisioning Profiles page, select the profile of interest and click Edit.

3 In the Provisioning Fields dialog box, click Microsoft Lync Settings and enter a Group Name.

   The Group Name is the group set in the Microsoft Lync Server or Office Communication Server.

4 Click OK.

Microsoft Directory Considerations

When Polycom endpoints are registered with a Microsoft Lync Server or Office Communications Sever, the SIP server replaces the RealPresence Resource Manager system as the presence and directory service provider. However, the system continues to act as manager for these endpoint systems.

If you want your directories to include endpoints such as CMA Desktop that are not registered to the Microsoft SIP server, you need to select Standard as your SIP server when provisioning settings.

You still need to use the RealPresence Resource Manager system provisioning credentials when provisioning the SIP settings to the endpoint.
Supported Endpoint Types

**Endpoint Types**

The following tables describe the Polycom® RealPresence® Resource Manager system support for endpoints based on endpoint type and category of support. See the *Polycom Resource Manager System Release Notes* for more information on tested and supported endpoint versions.

<table>
<thead>
<tr>
<th>Polycom Endpoint Types</th>
<th>Global Address Book Access</th>
<th>Dynamic Management</th>
<th>Standard Management</th>
<th>Scheduling (Dial in only)</th>
<th>Scheduling (Dial in and Dial out)</th>
<th>Monitoring (Standard)</th>
<th>Command and Control</th>
<th>Reports for IP Calls</th>
<th>Reports for ISDN Calls</th>
<th>Can be Managed Behind a Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealPresence Mobile</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>CMA Desktop</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>HDX Series (dynamic management mode)</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>HDX Series (standard management mode)</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>VVX Series (dynamic management mode)</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>VVX Series (standard management mode)</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>
### Polycom Endpoint Types

<table>
<thead>
<tr>
<th>Polycom Endpoint Types</th>
<th>Global Address Book Access</th>
<th>Dynamic Management</th>
<th>Standard Management</th>
<th>Scheduling (Dial in only)</th>
<th>Scheduling (Dial in and Dial out)</th>
<th>Monitoring (Standard)</th>
<th>Command and Control</th>
<th>Reports for IP Calls</th>
<th>Reports for ISDN Calls</th>
<th>Can be Managed Behind a Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSX Series</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>QDX Series</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Other Polycom endpoints:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- a. Dynamic Management and Standard Management are mutually exclusive functionality.
- b. Scheduling (Dial In Only) and Scheduling (Dial In and Dial Out) are presented as mutually exclusive functionality. Some endpoints, such as Polycom VVX systems do not have interfaces that can be ask to perform dialing. Some endpoints, such as CMA Desktop clients and VVX systems require external MCU resources for dial-in conferences.
- c. Standard RealPresence Resource Manager monitoring does not involve using SNMP. It includes endpoint monitoring (online/offline status) and alerts.
- d. Command and Control means the RealPresence Resource Manager system can send a command like Send Message and Reboot, and the endpoint can receive and act on the command.
- e. Reports for IP Calls are generated as part of standard gatekeeper functionality. Reports for ISDN Calls are additional system functionality. Endpoints that aren’t registered with the gatekeeper or ISDN calls send an alert to the device management function to record CDR information. Some legacy endpoints do not send this alert so the CDRs are not written.
- f. Supported behind a Polycom VBP device with Access Proxy enabled.
Some notes about the TANDBERG connection to the Global Address Book:

- Even if the Global Address Book is password protected, TANDBERG endpoints are not required to provide a password. They have unrestricted access to the Global Address Book.
A RealPresence Resource Manager system may also list an endpoint type of Other. The RealPresence Resource Manager system cannot manage endpoints with a type of Other and cannot direct these endpoints to initiate point-to-point calls. A scheduled point-to-point call between two endpoint systems with an endpoint type of Other requires the use of an MCU.

The Polycom RealPresence Mobility and Telepresence M100 systems register as endpoint type of Other. As such, the Resource Manager can schedule and perform limited monitoring of these systems.

For information about restrictions in changing passwords for a specific endpoint, see the documentation for the endpoint.

**Considerations for Third-Party Endpoints**

The RealPresence Resource Manager system includes additional command and control for select TANDBERG C Series, TANDBERG Edge, and LifeSize Team and Express endpoints. The RealPresence Resource Manager system can send a Reboot command to these endpoints, and the endpoints can receive and act on the command. In addition, the RealPresence Resource Manager system can:

- Discover these endpoints by searching for them within a range of IP addresses.
- Complete the initial provisioning of these endpoints.
- Schedule and launch point-to-point conferences on these endpoints.
- Launch the management interface for these endpoints.

In the following sections, some additional considerations for supporting third-party endpoints are discussed, including

- “Considerations for TANDBERG Endpoints” on page 165
- “Considerations for LifeSize Endpoints” on page 184
- “Reporting” on page 191
- “Monitoring” on page 191
Considerations for TANDBERG Endpoints

Enable TANDBERG Endpoints Global Address Book Access

With the RealPresence Resource Manager system, users of the TANDBERG 150, 990, 880, 770 MXP, TANDBERG C Series, and TANDBERG Edge can access the Polycom Global Address Book, so they can see the endpoints in the Global Address Book.

The timing of the endpoint’s connection with the Global Address Book can affect the success of its connection. We recommend the following process:

1. At the endpoint, enter the information required for directory set up including the Polycom Global Address Book/RealPresence Resource Manager system IP address and the path. To do this, on the endpoint, go to Endpoint Configuration > General > External Phone Book Settings.

2. Wait for the connections to take effect.

3. At the RealPresence Resource Manager system, go to Endpoint > Monitor View and verify the endpoint’s Global Address Book connection status is green.

Scheduled Provisioning of Selected TANDBERG Endpoints

The following table identifies the fields that the RealPresence Resource Manager system can provision for TANDBERG 150, 990, 880, and 770 MXP endpoints.

See the appropriate TANDBERG product documentation for more information about these fields and their acceptable values. See “Scheduled Provisioning of Endpoints” on page 143 for information on implementing scheduled provisioning of endpoints.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Provisioned for supported Tandberg models?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>AdditionalCamera Type</td>
<td>Y</td>
</tr>
<tr>
<td>AlertSpeaker Mode</td>
<td>Y</td>
</tr>
<tr>
<td>AlertTone Telephony</td>
<td>Y</td>
</tr>
<tr>
<td>AlertTone VideoTelephony</td>
<td>Y</td>
</tr>
<tr>
<td>AlertTone Volume</td>
<td>Y</td>
</tr>
<tr>
<td>AllowLatency</td>
<td>Y</td>
</tr>
<tr>
<td>Audio AGC</td>
<td>N</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>Audio AGC AUX</td>
<td>Y</td>
</tr>
<tr>
<td>Audio AGC Microphones</td>
<td>Y</td>
</tr>
<tr>
<td>Audio AGC Received</td>
<td>Y</td>
</tr>
<tr>
<td>Audio AGC VCR</td>
<td>Y</td>
</tr>
<tr>
<td>Audio AudioModule</td>
<td>Y</td>
</tr>
<tr>
<td>Audio AutoMute</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Delay AUX</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Delay VCR</td>
<td>Y</td>
</tr>
<tr>
<td>Audio EchoControl</td>
<td>N</td>
</tr>
<tr>
<td>Audio EchoControl 1 through 4</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Feedback Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Inputs Line 1 through 3 Level</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Inputs Line 1 through 3 Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Inputs Microphone 1 through 3</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Inputs Microphone 1 through 3 Level</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Inputs Microphone 1 through 3 Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Audio KeyTones</td>
<td>Y</td>
</tr>
<tr>
<td>Audio LocalDetection Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Loudspeaker</td>
<td>N</td>
</tr>
<tr>
<td>Audio MicrophoneMixer Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Microphones Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Outputs Line 1 through 3 Level</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Outputs Line 1 through 3 Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Outputs Line 1 through 3 Type</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Stereo</td>
<td>Y</td>
</tr>
<tr>
<td>Audio StereoSpeakers</td>
<td>Y</td>
</tr>
</tbody>
</table>
## Supported Endpoint Types

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Provisioned for supported Tandberg models?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>Audio VCRDucking</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Volume</td>
<td>Y</td>
</tr>
<tr>
<td>AutoAnswer Delay</td>
<td>Y</td>
</tr>
<tr>
<td>AutoAnswer Device</td>
<td>N</td>
</tr>
<tr>
<td>AutoAnswer Mode</td>
<td>Y</td>
</tr>
<tr>
<td>AutoLayout Mode</td>
<td>Y</td>
</tr>
<tr>
<td>AutoPIP Mode</td>
<td>Y</td>
</tr>
<tr>
<td>AutoPIP TimeOut</td>
<td>Y</td>
</tr>
<tr>
<td>Bonding Rebonding</td>
<td>Y</td>
</tr>
<tr>
<td>Bonding Timer</td>
<td>Y</td>
</tr>
<tr>
<td>CallManager Address</td>
<td>Y</td>
</tr>
<tr>
<td>CallVideoSource</td>
<td>Y</td>
</tr>
<tr>
<td>Cameras 1 through 13</td>
<td>Y</td>
</tr>
<tr>
<td>Backlight</td>
<td>Y</td>
</tr>
<tr>
<td>Brightness Level</td>
<td>Y</td>
</tr>
<tr>
<td>Brightness Mode</td>
<td>Y</td>
</tr>
<tr>
<td>DualVisca</td>
<td>Y</td>
</tr>
<tr>
<td>Focus Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Gamma Level</td>
<td>Y</td>
</tr>
<tr>
<td>Gamma Mode</td>
<td>Y</td>
</tr>
<tr>
<td>IR</td>
<td>Y</td>
</tr>
<tr>
<td>Mirror</td>
<td>Y</td>
</tr>
<tr>
<td>Whitebalance Level</td>
<td>Y</td>
</tr>
<tr>
<td>Whitebalance Mode</td>
<td>Y</td>
</tr>
<tr>
<td>CameraDVI Mode</td>
<td>Y</td>
</tr>
<tr>
<td>CameraSleep Mode</td>
<td>Y</td>
</tr>
<tr>
<td>CameraSwUpgrade</td>
<td>Y</td>
</tr>
<tr>
<td>CameraTracking Speed</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Conference AAC-LD</td>
<td></td>
</tr>
<tr>
<td>Conference AAC-LD-128-Mono</td>
<td></td>
</tr>
<tr>
<td>Conference AAC-LD-128-Threshold</td>
<td></td>
</tr>
<tr>
<td>Conference AIM</td>
<td></td>
</tr>
<tr>
<td>Conference AllowIncomingCallInCall</td>
<td></td>
</tr>
<tr>
<td>Conference AllowIncomingMSCall</td>
<td></td>
</tr>
<tr>
<td>Conference AllowIncomingTlphCall</td>
<td></td>
</tr>
<tr>
<td>Conference BillingCode</td>
<td></td>
</tr>
<tr>
<td>Conference DefaultCall CallRate</td>
<td></td>
</tr>
<tr>
<td>Conference DefaultCall NetProfile</td>
<td></td>
</tr>
<tr>
<td>Conference DefaultCall Restrict</td>
<td></td>
</tr>
<tr>
<td>Conference Downspeed</td>
<td></td>
</tr>
<tr>
<td>Conference Encryption Mode</td>
<td></td>
</tr>
<tr>
<td>Conference Encryption Type</td>
<td></td>
</tr>
<tr>
<td>Conference FallbackToTelephony</td>
<td></td>
</tr>
<tr>
<td>Conference FarTlphEchoSupression</td>
<td></td>
</tr>
<tr>
<td>Conference FloorToFull</td>
<td></td>
</tr>
<tr>
<td>Conference G722</td>
<td></td>
</tr>
<tr>
<td>Conference G722.1</td>
<td></td>
</tr>
<tr>
<td>Conference G728</td>
<td></td>
</tr>
<tr>
<td>Conference H239</td>
<td></td>
</tr>
<tr>
<td>Conference H263</td>
<td></td>
</tr>
<tr>
<td>Conference H264</td>
<td></td>
</tr>
<tr>
<td>Conference H264RCDO</td>
<td></td>
</tr>
<tr>
<td>Conference H331</td>
<td></td>
</tr>
<tr>
<td>Conference IPDualstreamRate</td>
<td></td>
</tr>
<tr>
<td>Conference IPLR Transmit</td>
<td></td>
</tr>
<tr>
<td>Conference MailBox URI</td>
<td></td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>MXP Models 990/880/770</strong></td>
</tr>
<tr>
<td>Conference MaxCallLength</td>
<td>Y</td>
</tr>
<tr>
<td>Conference NaturalVideo</td>
<td>Y</td>
</tr>
<tr>
<td>Conference PeriodicIntra</td>
<td>Y</td>
</tr>
<tr>
<td>Conference PictureMode</td>
<td>Y</td>
</tr>
<tr>
<td>Conference SIP URI</td>
<td>N</td>
</tr>
<tr>
<td>Conference VideoQualityCP</td>
<td>Y</td>
</tr>
<tr>
<td>Conference VideoText</td>
<td>Y</td>
</tr>
<tr>
<td>Conference VideoTextTimeout</td>
<td>Y</td>
</tr>
<tr>
<td>Conference WebSnapshots</td>
<td>Y</td>
</tr>
<tr>
<td>CorporateDirectory Address</td>
<td>Y</td>
</tr>
<tr>
<td>CorporateDirectory Mode</td>
<td>Y</td>
</tr>
<tr>
<td>CorporateDirectory Path</td>
<td>Y</td>
</tr>
<tr>
<td>CorporateDirectory Protocol</td>
<td>Y</td>
</tr>
<tr>
<td>DefaultPIPPosition</td>
<td>Y</td>
</tr>
<tr>
<td>Directory CallLog</td>
<td>Y</td>
</tr>
<tr>
<td>Directory SmartSearch</td>
<td>Y</td>
</tr>
<tr>
<td>DoNotDisturb Mode</td>
<td>Y</td>
</tr>
<tr>
<td>DualMonitor Mode</td>
<td>Y</td>
</tr>
<tr>
<td>DuoVideoSource</td>
<td>Y</td>
</tr>
<tr>
<td>DynamicResolution Mode</td>
<td>Y</td>
</tr>
<tr>
<td>E1 Interface CRC4</td>
<td>Y</td>
</tr>
<tr>
<td>Ethernet 1 Speed</td>
<td>Y</td>
</tr>
<tr>
<td>Ethernet 2 Speed</td>
<td>Y</td>
</tr>
<tr>
<td>ExternalNetwork Callcontroll</td>
<td>Y</td>
</tr>
<tr>
<td>ExternalNetwork Clocking</td>
<td>Y</td>
</tr>
<tr>
<td>ExternalNetwork DTRPulse</td>
<td>Y</td>
</tr>
<tr>
<td>ExternalServices Address</td>
<td>Y</td>
</tr>
<tr>
<td>ExternalServices Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>ExternalServices Path</td>
<td>Y</td>
</tr>
<tr>
<td>ExternalServices Protocol</td>
<td>Y</td>
</tr>
<tr>
<td>FECC Mode</td>
<td>Y</td>
</tr>
<tr>
<td>FeedbackFilter Call</td>
<td>Y</td>
</tr>
<tr>
<td>FeedbackFilter Conference</td>
<td>Y</td>
</tr>
<tr>
<td>FTP Mode</td>
<td>Y</td>
</tr>
<tr>
<td>G703 Callcontrol</td>
<td>Y</td>
</tr>
<tr>
<td>G703 Interface MaxChannels</td>
<td>Y</td>
</tr>
<tr>
<td>G703 Interface StartChannel</td>
<td>Y</td>
</tr>
<tr>
<td>G703 Linecoding</td>
<td>Y</td>
</tr>
<tr>
<td>G703 PhysicalLayer</td>
<td>Y</td>
</tr>
<tr>
<td>H320 NetType</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Mode</td>
<td>Y</td>
</tr>
<tr>
<td>H323 CallSetup Mode</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Address</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Authentication ID</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Authentication Mode</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Authentication Password</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Avaya AnnexH</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Avaya Mode</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Avaya MultipointCount</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Avaya Password</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper Discovery</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Gatekeeper MultipleAlias</td>
<td>Y</td>
</tr>
<tr>
<td>H323 Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>HTTP Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>HTTPS Mode</td>
<td></td>
</tr>
<tr>
<td>HTTPS VerifyServerCertificate</td>
<td></td>
</tr>
<tr>
<td>IdReport H323</td>
<td></td>
</tr>
<tr>
<td>IEEE802.1x AnonymousIdentity</td>
<td></td>
</tr>
<tr>
<td>IEEE802.1x EAP-MD5</td>
<td></td>
</tr>
<tr>
<td>IEEE802.1x EAP-PEAP</td>
<td></td>
</tr>
<tr>
<td>IEEE802.1x EAP-TTLS</td>
<td></td>
</tr>
<tr>
<td>IEEE802.1x Identity</td>
<td></td>
</tr>
<tr>
<td>IEEE802.1x Mode</td>
<td></td>
</tr>
<tr>
<td>IEEE802.1x Password</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1152 Prefix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1152 Suffix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1152R Prefix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1152R Suffix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw128 Prefix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw128 Suffix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw128R Prefix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw128R Suffix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1472 Prefix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1472 Suffix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1472R Prefix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1472R Suffix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw192 Prefix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw192 Suffix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1920R Prefix</td>
<td></td>
</tr>
<tr>
<td>IMUX Custom bw1920R Suffix</td>
<td></td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>IMUX Custom bw192R Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw192R Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw256 Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw256 Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw256R Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw256R Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw320 Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw320 Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw320R Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw320R Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw384 Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw384 Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw384R Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw384R Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw512 Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw512 Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw512R Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw512R Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw64 Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw64 Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw64R Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw64R Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw768 Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw768 Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw768R Prefix</td>
<td>Y</td>
</tr>
<tr>
<td>IMUX Custom bw768R Suffix</td>
<td>Y</td>
</tr>
<tr>
<td>Integrator AMXBeacon Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Integrator Telepresence Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>IP Assignment</td>
<td>Y</td>
</tr>
<tr>
<td>IP DNS Domain Name</td>
<td>Y</td>
</tr>
<tr>
<td>IP DNS Server 1 through 5 Address</td>
<td>Y</td>
</tr>
<tr>
<td>IP Gateway</td>
<td>Y</td>
</tr>
<tr>
<td>IP SubnetMask</td>
<td>Y</td>
</tr>
<tr>
<td>IPMedia MaxVideoTXRate</td>
<td>Y</td>
</tr>
<tr>
<td>IPProtocol</td>
<td>Y</td>
</tr>
<tr>
<td>IRControl Mode</td>
<td>Y</td>
</tr>
<tr>
<td>IRControl NumberKeyMode</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN BRI Alert</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN BRI AutoActivation</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN BRI ChanId</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN BRI Interface 1 through 6</td>
<td>Y</td>
</tr>
<tr>
<td>DirectoryNumber 1</td>
<td>Y</td>
</tr>
<tr>
<td>DirectoryNumber 2</td>
<td>Y</td>
</tr>
<tr>
<td>Mode</td>
<td>Y</td>
</tr>
<tr>
<td>SPID 1</td>
<td>Y</td>
</tr>
<tr>
<td>SPID 2</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN BRI MaxDeactiveTime</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN BRI SwitchType</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN CliNumbPlan</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN CliNumbSpec</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN CliNumbType</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN HLC</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN MSN</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN ParallelDial</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI Alert</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI ChanId</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>ISDN PRI InitialRestart</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI Interface HighChannel</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI Interface LowChannel</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI Interface MaxChannels</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI Interface NumberRangeStart</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI Interface NumberRangeStop</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI Interface Search</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI L2WindowSize</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI NSFTelephony Mode</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI NSFTelephony Number</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI NSFVideoTelephony Mode</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI NSFVideoTelephony Number</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN PRI SwitchType</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN SendComplete</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN SendNumber</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN SpeechTimers</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN SubAddress</td>
<td>Y</td>
</tr>
<tr>
<td>Key AUX</td>
<td>Y</td>
</tr>
<tr>
<td>Key Brightness</td>
<td>N</td>
</tr>
<tr>
<td>Key Cabinet</td>
<td>Y</td>
</tr>
<tr>
<td>Key CallRegister</td>
<td>N</td>
</tr>
<tr>
<td>Key Cancel</td>
<td>Y</td>
</tr>
<tr>
<td>Key Connect</td>
<td>Y</td>
</tr>
<tr>
<td>Key Disconnect</td>
<td>Y</td>
</tr>
<tr>
<td>Key DocCam</td>
<td>Y</td>
</tr>
<tr>
<td>Key Down</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Key FarEnd</td>
<td>Y</td>
</tr>
<tr>
<td>Key Grab</td>
<td>Y</td>
</tr>
<tr>
<td>Key Headset</td>
<td>N</td>
</tr>
<tr>
<td>Key Help</td>
<td>Y</td>
</tr>
<tr>
<td>Key Layout</td>
<td>Y</td>
</tr>
<tr>
<td>Key Left</td>
<td>Y</td>
</tr>
<tr>
<td>Key MainCam</td>
<td>Y</td>
</tr>
<tr>
<td>Key MicOff</td>
<td>Y</td>
</tr>
<tr>
<td>Key Number0 through Number9</td>
<td>Y</td>
</tr>
<tr>
<td>Key Ok</td>
<td>Y</td>
</tr>
<tr>
<td>Key PC</td>
<td>Y</td>
</tr>
<tr>
<td>Key Phonebook</td>
<td>Y</td>
</tr>
<tr>
<td>Key PIP</td>
<td>N</td>
</tr>
<tr>
<td>Key Presentation</td>
<td>Y</td>
</tr>
<tr>
<td>Key Presets</td>
<td>Y</td>
</tr>
<tr>
<td>Key Right</td>
<td>Y</td>
</tr>
<tr>
<td>Key Selfview</td>
<td>Y</td>
</tr>
<tr>
<td>Key Services</td>
<td>Y</td>
</tr>
<tr>
<td>Key Settings</td>
<td>N</td>
</tr>
<tr>
<td>Key Softkey1</td>
<td>N</td>
</tr>
<tr>
<td>Key Softkey2</td>
<td>N</td>
</tr>
<tr>
<td>Key Softkey3</td>
<td>N</td>
</tr>
<tr>
<td>Key Softkey4</td>
<td>N</td>
</tr>
<tr>
<td>Key Softkey5</td>
<td>N</td>
</tr>
<tr>
<td>Key Speaker</td>
<td>N</td>
</tr>
<tr>
<td>Key Square</td>
<td>Y</td>
</tr>
<tr>
<td>Key Star</td>
<td>Y</td>
</tr>
<tr>
<td>Key Up</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>Key VideoOff</td>
<td>N</td>
</tr>
<tr>
<td>Key VCR</td>
<td>Y</td>
</tr>
<tr>
<td>Key VolumeDown</td>
<td>Y</td>
</tr>
<tr>
<td>Key VolumeUp</td>
<td>Y</td>
</tr>
<tr>
<td>Key ZoomIn</td>
<td>Y</td>
</tr>
<tr>
<td>Key ZoomOut</td>
<td>Y</td>
</tr>
<tr>
<td>Keyboard Layout</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk AllowIRControl</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk AutoDial</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk LanguageMenu English</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk LanguageMenu French</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk LanguageMenu German</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk LanguageMenu Italian</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk LanguageMenu Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk LanguageMenu Norwegian</td>
<td></td>
</tr>
<tr>
<td>Kiosk LanguageMenu Spanish</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk LanguageMenu Swedish</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk Menu</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk OneClickConnect</td>
<td>Y</td>
</tr>
<tr>
<td>Kiosk Phonebook</td>
<td>Y</td>
</tr>
<tr>
<td>LocalLayout Mode</td>
<td>Y</td>
</tr>
<tr>
<td>LocalLayout Toggle</td>
<td>Y</td>
</tr>
<tr>
<td>Logo</td>
<td>Y</td>
</tr>
<tr>
<td>LoS Duration Exponent</td>
<td>Y</td>
</tr>
<tr>
<td>LoS Duration Offset</td>
<td>Y</td>
</tr>
<tr>
<td>LoS Inhibit</td>
<td>Y</td>
</tr>
<tr>
<td>LoS Initial</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>LoS Polarity</td>
<td>Y</td>
</tr>
<tr>
<td>LoS Retry</td>
<td>Y</td>
</tr>
<tr>
<td>MainVideoSource</td>
<td>Y</td>
</tr>
<tr>
<td>MaxBandwidth</td>
<td>Y</td>
</tr>
<tr>
<td>Multipoint Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Multipoint MultiwayMultiProtocol</td>
<td>Y</td>
</tr>
<tr>
<td>Multipoint MultiwayStartupPeriod</td>
<td>Y</td>
</tr>
<tr>
<td>Multipoint MultiwayURI</td>
<td>Y</td>
</tr>
<tr>
<td>NAT Address</td>
<td>Y</td>
</tr>
<tr>
<td>NAT Mode</td>
<td>Y</td>
</tr>
<tr>
<td>NetProfile 1 through 7</td>
<td>Y</td>
</tr>
<tr>
<td>CallPrefix</td>
<td>Y</td>
</tr>
<tr>
<td>CallSuffix</td>
<td>Y</td>
</tr>
<tr>
<td>Name</td>
<td>Y</td>
</tr>
<tr>
<td>NTP Address</td>
<td>Y</td>
</tr>
<tr>
<td>NTP Mode</td>
<td>Y</td>
</tr>
<tr>
<td>OneClickConnect Mode</td>
<td>N</td>
</tr>
<tr>
<td>OSD CallDuration Mode</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon BadNetwork</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon CameraTracking</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon DuoVideo</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon Encryption</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon Headset</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon MicOff</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon OnAir</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon Telephone</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Icon VolumeOff</td>
<td>Y</td>
</tr>
<tr>
<td>OSD MCUStatusLine Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>OSD Menu BalloonHelp</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu CodecLabel</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu DisableH323IdCalling</td>
<td>N</td>
</tr>
<tr>
<td>OSD Menu DisableTimeout</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu DisplayWelcomeText</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu DisplayWelcomeTime</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu IconPlacement</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu InputEditor Language</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu Language</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu Mode</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu Password</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu Simple</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu WelcomeMenu</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Menu WelcomeText</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Mode</td>
<td>Y</td>
</tr>
<tr>
<td>OSD Offset Mode</td>
<td>Y</td>
</tr>
<tr>
<td>PacketlossDownSpeed Mode</td>
<td>Y</td>
</tr>
<tr>
<td>PCPort Mode</td>
<td>N</td>
</tr>
<tr>
<td>PictureProgram 1 Layout</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 1 Window 1 through 6 Call</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 1 Window 1 through 6 Picture</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 2 Layout</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 2 Window 1 through 6 Call</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 2 Window 1 through 6 Picture</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 3 Layout</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>PictureProgram 3 Window 1 through 6 Call</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 3 Window 1 through 6 Picture</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 4 Layout</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 4 Window 1 through 6 Call</td>
<td>Y</td>
</tr>
<tr>
<td>PictureProgram 4 Window 1 through 6 Picture</td>
<td>Y</td>
</tr>
<tr>
<td>PresentationStart</td>
<td>Y</td>
</tr>
<tr>
<td>Preset 1 through 15 Name</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Diffserv Telephony Audio</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Diffserv Telephony Signalling</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Diffserv VideoTelephony Audio</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Diffserv VideoTelephony Data</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Diffserv VideoTelephony Signalling</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Diffserv VideoTelephony Video</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Mode</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Precedence Telephony Audio</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Precedence Telephony Signalling</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Precedence VideoTelephony Audio</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Precedence VideoTelephony Data</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Precedence VideoTelephony Signalling</td>
<td>Y</td>
</tr>
<tr>
<td>QoS Precedence VideoTelephony Video</td>
<td>Y</td>
</tr>
<tr>
<td>QoS RSVP</td>
<td>Y</td>
</tr>
<tr>
<td>QoS ToS</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>RemoteSwUpgrade Mode</td>
<td>Y</td>
</tr>
<tr>
<td>RemoteSwUpgrade Password</td>
<td>Y</td>
</tr>
<tr>
<td>RTP MTU</td>
<td>Y</td>
</tr>
<tr>
<td>RTP Ports</td>
<td>Y</td>
</tr>
<tr>
<td>Screensaver Delay</td>
<td>Y</td>
</tr>
<tr>
<td>Screensaver LED</td>
<td>N</td>
</tr>
<tr>
<td>Screensaver Mode</td>
<td>Y</td>
</tr>
<tr>
<td>SecurityLog Mode</td>
<td>Y</td>
</tr>
<tr>
<td>SelfViewOnStartup</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 1 BaudRate</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 1 DataBits</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 1 Mode</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 1 Parity</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 1 StopBits</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 2 BaudRate</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 2 DataBits</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 2 Mode</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 2 Parity</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort 2 StopBits</td>
<td>Y</td>
</tr>
<tr>
<td>SerialPort Direct Buffer</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Authentication Password</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Authentication UserName</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Legacy Mask</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Mode</td>
<td>Y</td>
</tr>
<tr>
<td>SIP ReplyTo URI</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Server Address</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Server Discovery</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Server Type</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>SIP TLS Verify</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Transport Default</td>
<td>Y</td>
</tr>
<tr>
<td>SNMP CommunityName</td>
<td>Y</td>
</tr>
<tr>
<td>SNMP HostIPAddr 1</td>
<td>Y</td>
</tr>
<tr>
<td>SNMP HostIPAddr 2</td>
<td>Y</td>
</tr>
<tr>
<td>SNMP HostIPAddr 3</td>
<td>Y</td>
</tr>
<tr>
<td>SNMP Mode</td>
<td>Y</td>
</tr>
<tr>
<td>SNMP SystemContact</td>
<td>Y</td>
</tr>
<tr>
<td>SNMP SystemLocation</td>
<td>Y</td>
</tr>
<tr>
<td>SSH Mode</td>
<td>Y</td>
</tr>
<tr>
<td>StartupVideoSource</td>
<td>Y</td>
</tr>
<tr>
<td>StillImageSource</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming Address</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming AllowRemoteStart</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming Announcements</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming Hops</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming Password</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming Port</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming Quality</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming Source</td>
<td>Y</td>
</tr>
<tr>
<td>Streaming VideoRate</td>
<td>Y</td>
</tr>
<tr>
<td>StrictPassword</td>
<td>Y</td>
</tr>
<tr>
<td>Switch Configuration Primary</td>
<td>Y</td>
</tr>
<tr>
<td>Switch Configuration Secondary</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 1 Map</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 1 Mode 1</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 1 Mode 2</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 1 Mode 3</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>Switch LogicalInput 1 Mode 4</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 1 Mode 5</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 2 Map</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 2 Mode 1</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 3 Map</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 3 Mode 1</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 4 Map</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 4 Mode 1</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 5 Map</td>
<td>Y</td>
</tr>
<tr>
<td>Switch LogicalInput 5 Mode 1</td>
<td>Y</td>
</tr>
<tr>
<td>Switch Source</td>
<td>Y</td>
</tr>
<tr>
<td>SystemUnit Multiway</td>
<td>N</td>
</tr>
<tr>
<td>SystemUnit Password</td>
<td>Y</td>
</tr>
<tr>
<td>T1 Interface CableLength</td>
<td>Y</td>
</tr>
<tr>
<td>Telnet Mode</td>
<td>Y</td>
</tr>
<tr>
<td>TelnetChallenge Mode</td>
<td>Y</td>
</tr>
<tr>
<td>TelnetChallenge Port</td>
<td>Y</td>
</tr>
<tr>
<td>Time DateFormat</td>
<td>Y</td>
</tr>
<tr>
<td>Time DaylightSavings</td>
<td>Y</td>
</tr>
<tr>
<td>Time TimeFormat</td>
<td>Y</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Y</td>
</tr>
<tr>
<td>UseAsLocalPCMonitor</td>
<td>Y</td>
</tr>
<tr>
<td>Video 1 Outputs Animation</td>
<td>Y</td>
</tr>
<tr>
<td>Video 1 Outputs Testpattern</td>
<td>Y</td>
</tr>
<tr>
<td>Video Inputs Source 1 through 6</td>
<td>Y</td>
</tr>
<tr>
<td>Name</td>
<td>Y</td>
</tr>
<tr>
<td>Quality</td>
<td>Y</td>
</tr>
<tr>
<td>Video Outputs DVI 1 and 2</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for supported Tandberg models?</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>MXP Models 990/880/770</td>
</tr>
<tr>
<td>Mode</td>
<td>Y</td>
</tr>
<tr>
<td>OSD</td>
<td>Y</td>
</tr>
<tr>
<td>VirtualMonitor</td>
<td>Y</td>
</tr>
<tr>
<td>Video Outputs DVIResolution</td>
<td>Y</td>
</tr>
<tr>
<td>Video Outputs Letterbox</td>
<td>Y</td>
</tr>
<tr>
<td>Video Outputs ScreenFormatPC</td>
<td>Y</td>
</tr>
<tr>
<td>Video Outputs ScreenFormatTV</td>
<td>Y</td>
</tr>
<tr>
<td>Video Outputs TV 1 and 2</td>
<td>Y</td>
</tr>
<tr>
<td>Mode</td>
<td>Y</td>
</tr>
<tr>
<td>OSD</td>
<td>Y</td>
</tr>
<tr>
<td>VirtualMonitor</td>
<td>Y</td>
</tr>
<tr>
<td>VNC DisplayNumber</td>
<td>Y</td>
</tr>
<tr>
<td>VNC IPAddress</td>
<td>Y</td>
</tr>
<tr>
<td>VNC Password</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN Community</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN Enable</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN Encryption</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN Key 1</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN Key 2</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN Key 3</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN Key 4</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN Mode</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN SSID</td>
<td>Y</td>
</tr>
<tr>
<td>WLAN UseKey</td>
<td>Y</td>
</tr>
</tbody>
</table>

a. The RealPresenceResource Manager system always provisions Telnet Mode to ON, because provisioning Telnet Mode to OFF would make the endpoints unmanageable.
Considerations for LifeSize Endpoints

Consider the following when you must support LifeSize endpoints:

- “Enabling Management of a LifeSize Endpoints” on page 184
- “Provisioning of LifeSize Passwords” on page 184
- “Scheduled Provisioning of LifeSize Endpoints” on page 185

Enabling Management of a LifeSize Endpoints

To facilitate management of a LifeSize endpoint, you must enable the Default Passwords for LifeSize Endpoint Management option and enter the SSH and web UI passwords for the LifeSize endpoints.

To enable LifeSize endpoint management


3. Enter the Password for SSH User and confirm the password. Refer to the LifeSize system documentation for information on using SSH to connect to the endpoint, then enter the same SSH password here.

4. Enter the Password for Web UI User and confirm the password. Refer to the LifeSize system documentation for information on using a web browser to connect to the endpoint, then enter the same web UI password here.

5. Click Update.

Provisioning of LifeSize Passwords

Take note of the following when provisioning passwords to LifeSize endpoints:

- The Auto password must be provisioned to meet the LifeSize and SSH/telnet rules for passwords.
- You cannot provision the Auto password to be blank. If you attempt to provision a blank value, the existing value of the password will not be overwritten. It will remain valid.
- The Web UI or User password can be provisioned to include the numbers 0-9 and/or the symbols * and #. The system will silently truncate these passwords to a maximum of 16 characters.
- You can provision the Web UI or User password to be blank.
Refer to the LifeSize documentation for more information about the requirements for these passwords.

**Scheduled Provisioning of LifeSize Endpoints**

The RealPresence Resource Manager system can provision many fields for LifeSize Team and Express endpoints. The following table identifies the fields that the RealPresence Resource Manager system can provision for LifeSize Team 200 endpoints. See the “Scheduled Provisioning of Endpoints” on page 143 for information on implementing scheduled provisioning of endpoints.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Provisioned for selected LifeSize Models?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Calls</strong></td>
<td></td>
</tr>
<tr>
<td>Outgoing Max BandWidth</td>
<td>Y</td>
</tr>
<tr>
<td>Incoming Max BandWidth</td>
<td>Y</td>
</tr>
<tr>
<td>Auto Bandwidth</td>
<td>Y</td>
</tr>
<tr>
<td>Maximum Call Time</td>
<td>Y</td>
</tr>
<tr>
<td>Maximum Redial Entries</td>
<td>Y</td>
</tr>
<tr>
<td>Auto Answer</td>
<td>Y</td>
</tr>
<tr>
<td>Auto Answer Mute</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Audio</strong></td>
<td></td>
</tr>
<tr>
<td>Audio Codecs</td>
<td>Y</td>
</tr>
<tr>
<td>Active Microphone</td>
<td>Y</td>
</tr>
<tr>
<td>Active Microphone Volume</td>
<td>Y</td>
</tr>
<tr>
<td>Primary Audio Output Test</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Mute</td>
<td>Y</td>
</tr>
<tr>
<td>Muted Device(s)</td>
<td>Y</td>
</tr>
<tr>
<td>Video Call Audio Output</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Call Audio Output</td>
<td>Y</td>
</tr>
<tr>
<td>Line Out Treble</td>
<td>Y</td>
</tr>
<tr>
<td>Line Out Bass</td>
<td>Y</td>
</tr>
<tr>
<td>Ring Tone Volume</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for selected LifeSize Models?</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>DMF Tone Volume</td>
<td>Y</td>
</tr>
<tr>
<td>Status Tone Volume</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Telepresence</strong></td>
<td></td>
</tr>
<tr>
<td>Telepresence</td>
<td>Y</td>
</tr>
<tr>
<td>HD Camera 1 Moment</td>
<td>Y</td>
</tr>
<tr>
<td>HD Camera 2 Moment</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Video Settings &gt; Video Control</strong></td>
<td></td>
</tr>
<tr>
<td>Far Ctrl of Near Camera</td>
<td>Y</td>
</tr>
<tr>
<td>Far Set of Camera Presets</td>
<td>Y</td>
</tr>
<tr>
<td>Far Move to Camera Presets</td>
<td>Y</td>
</tr>
<tr>
<td>Camera Presets Lock</td>
<td>Y</td>
</tr>
<tr>
<td>Camera Pan Direction</td>
<td>Y</td>
</tr>
<tr>
<td>Default Primary Input</td>
<td>Y</td>
</tr>
<tr>
<td>Video Snapshots</td>
<td>Y</td>
</tr>
<tr>
<td>HD Camera 1 Name</td>
<td>Y</td>
</tr>
<tr>
<td>HD Input 1 Name</td>
<td>Y</td>
</tr>
<tr>
<td>Stretch Video</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Video Settings &gt; Video Quality</strong></td>
<td></td>
</tr>
<tr>
<td>Video Bandwidth Balance</td>
<td>Y</td>
</tr>
<tr>
<td>Primary Video Motion</td>
<td>Y</td>
</tr>
<tr>
<td>Presentation Video Sharpness</td>
<td>Y</td>
</tr>
<tr>
<td>Video Encoder Quality</td>
<td>Y</td>
</tr>
<tr>
<td>H.241 MaxStaticMBPS</td>
<td>Y</td>
</tr>
<tr>
<td>Video MTU</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Security &gt; General</strong></td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Y</td>
</tr>
<tr>
<td>SNMP</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Security &gt; Passwords</strong></td>
<td></td>
</tr>
<tr>
<td>SSH Password</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for selected LifeSize Models?</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>UI Admin Password</td>
<td>Y</td>
</tr>
<tr>
<td>UI User Password</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Network &gt; General</strong></td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>Y</td>
</tr>
<tr>
<td>IP Address</td>
<td>Y</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Y</td>
</tr>
<tr>
<td>Gateway</td>
<td>Y</td>
</tr>
<tr>
<td>Host Name</td>
<td>Y</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Y</td>
</tr>
<tr>
<td>Name Search Domains</td>
<td>Y</td>
</tr>
<tr>
<td>Network Speed</td>
<td>Y</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>Y</td>
</tr>
<tr>
<td>NTP Server Host Name</td>
<td>Y</td>
</tr>
<tr>
<td>802.1x Authentication</td>
<td>Y</td>
</tr>
<tr>
<td>IPv6 Configuration</td>
<td>Y</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Y</td>
</tr>
<tr>
<td>IPv6 Router</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Network &gt; NAT</strong></td>
<td></td>
</tr>
<tr>
<td>Static NAT</td>
<td>Y</td>
</tr>
<tr>
<td>NAT Public IP Address</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Network &gt; Reserved Ports</strong></td>
<td></td>
</tr>
<tr>
<td>UDP Lowest Value</td>
<td>Y</td>
</tr>
<tr>
<td>UDP Highest Value</td>
<td>Y</td>
</tr>
<tr>
<td>TCP Highest Value</td>
<td>Y</td>
</tr>
<tr>
<td>TCP Lowest Value</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Network &gt; Network Qos</strong></td>
<td></td>
</tr>
<tr>
<td>Network QoS</td>
<td>Y</td>
</tr>
<tr>
<td>DiffServ Audio Priority</td>
<td>Y</td>
</tr>
<tr>
<td>DiffServ Video Priority</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for selected LifeSize Models?</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Team 200</td>
</tr>
<tr>
<td>DiffServ Data Priority</td>
<td>Y</td>
</tr>
<tr>
<td>InServ Audio Priority</td>
<td>Y</td>
</tr>
<tr>
<td>InServ Video Priority</td>
<td>Y</td>
</tr>
<tr>
<td>InServ Data Priority</td>
<td>Y</td>
</tr>
<tr>
<td>InServ ToS</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Network &gt; LifeSize® Transit</strong></td>
<td></td>
</tr>
<tr>
<td>LifeSize® Transit</td>
<td>Y</td>
</tr>
<tr>
<td>Transit Hostname</td>
<td>Y</td>
</tr>
<tr>
<td>Transit Username</td>
<td>Y</td>
</tr>
<tr>
<td>Transit Password</td>
<td>Y</td>
</tr>
<tr>
<td>Transit ICE</td>
<td>Y</td>
</tr>
<tr>
<td>Transit Signaling</td>
<td>Y</td>
</tr>
<tr>
<td>Web Proxy URL</td>
<td>Y</td>
</tr>
<tr>
<td>Web Proxy Username</td>
<td>Y</td>
</tr>
<tr>
<td>Web Proxy Password</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Communications &gt; General</strong></td>
<td></td>
</tr>
<tr>
<td>Auto Answer Multiway Calls</td>
<td>Y</td>
</tr>
<tr>
<td>Video Dialing</td>
<td>Y</td>
</tr>
<tr>
<td>Voice Dialing</td>
<td>Y</td>
</tr>
<tr>
<td>Presentations</td>
<td>Y</td>
</tr>
<tr>
<td>Auto Start Presentations</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Communications &gt; H.323</strong></td>
<td></td>
</tr>
<tr>
<td>H.323</td>
<td>Y</td>
</tr>
<tr>
<td>H.323 Name</td>
<td>Y</td>
</tr>
<tr>
<td>H.323 Extension</td>
<td>Y</td>
</tr>
<tr>
<td>Gatekeeper ID</td>
<td>Y</td>
</tr>
<tr>
<td>Gatekeeper Mode</td>
<td>Y</td>
</tr>
<tr>
<td>Primary Gatekeeper IP and Port</td>
<td>Y</td>
</tr>
<tr>
<td>Alternate Gatekeeper IP and Port</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for selected LifeSize Models?</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>H.460</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Communications &gt; SIP</strong></td>
<td></td>
</tr>
<tr>
<td>SIP</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Username</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Authorization</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Server Type</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Registration</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Proxy</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Proxy Host Name</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Proxy Port</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Registrar</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Registrar Host Name</td>
<td>Y</td>
</tr>
<tr>
<td>SIP Registrar Port</td>
<td>Y</td>
</tr>
<tr>
<td>UDP Signaling</td>
<td>Y</td>
</tr>
<tr>
<td>UDP Signaling Port</td>
<td>Y</td>
</tr>
<tr>
<td>TCP Signaling</td>
<td>Y</td>
</tr>
<tr>
<td>TCP Signaling Port</td>
<td>Y</td>
</tr>
<tr>
<td>TLS Signaling</td>
<td>Y</td>
</tr>
<tr>
<td>TLS Signaling Port</td>
<td>Y</td>
</tr>
<tr>
<td><strong>System &gt; General</strong></td>
<td></td>
</tr>
<tr>
<td>Auto Reboot</td>
<td>Y</td>
</tr>
<tr>
<td>System &gt; Identification</td>
<td>N</td>
</tr>
<tr>
<td>System Name</td>
<td>Y</td>
</tr>
<tr>
<td>Video Number</td>
<td>Y</td>
</tr>
<tr>
<td>Voice Number</td>
<td>Y</td>
</tr>
<tr>
<td><strong>System &gt; Identification</strong></td>
<td></td>
</tr>
<tr>
<td>Timezone</td>
<td>Y</td>
</tr>
<tr>
<td>Month</td>
<td>Y</td>
</tr>
<tr>
<td>Day</td>
<td>Y</td>
</tr>
<tr>
<td>Field Name</td>
<td>Provisioned for selected LifeSize Models?</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Team 200</td>
</tr>
<tr>
<td>Year</td>
<td>Y</td>
</tr>
<tr>
<td>Hour</td>
<td>Y</td>
</tr>
<tr>
<td>Minute</td>
<td>Y</td>
</tr>
<tr>
<td>Second</td>
<td>Y</td>
</tr>
<tr>
<td>Directory &gt; Auto Discovery</td>
<td></td>
</tr>
<tr>
<td>Auto Discovery</td>
<td>Y</td>
</tr>
<tr>
<td>Auto Discovery Subnets</td>
<td>Y</td>
</tr>
<tr>
<td>Auto Discovery Ignored Subnets</td>
<td>Y</td>
</tr>
<tr>
<td>Directory &gt; LDAP</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Y</td>
</tr>
<tr>
<td>LDAP Hostname</td>
<td>Y</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>Y</td>
</tr>
<tr>
<td>LDAP Base</td>
<td>Y</td>
</tr>
<tr>
<td>LDAP Filter</td>
<td>Y</td>
</tr>
<tr>
<td>LDAP Refresh</td>
<td>Y</td>
</tr>
<tr>
<td>Appearance &gt; General</td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>Y</td>
</tr>
<tr>
<td>Fade Out Timeout</td>
<td>Y</td>
</tr>
<tr>
<td>Company Logo</td>
<td>Y</td>
</tr>
<tr>
<td>LCD Contrast</td>
<td>Y</td>
</tr>
<tr>
<td>Screen Saver</td>
<td>Y</td>
</tr>
<tr>
<td>Screen Saver Timeout</td>
<td>Y</td>
</tr>
<tr>
<td>Sleep Timeout</td>
<td>Y</td>
</tr>
<tr>
<td>Appearance &gt; Layout</td>
<td></td>
</tr>
<tr>
<td>Picture in Picture</td>
<td>Y</td>
</tr>
<tr>
<td>Display 2 Layout</td>
<td>Y</td>
</tr>
<tr>
<td>Appearance &gt; Display</td>
<td></td>
</tr>
<tr>
<td>Display 1 Resolution</td>
<td>Y</td>
</tr>
<tr>
<td>Display 1 Energy Saver</td>
<td>Y</td>
</tr>
</tbody>
</table>
The RealPresence Resource Manager system includes standard reporting for select TANDBERG C Series, TANDBERG Edge, and LifeSize Team and Express endpoints.

**Reporting**

The RealPresence Resource Manager system can monitor select TANDBERG C Series, TANDBERG Edge, and LifeSize Team and Express endpoints, so when properly configured, the RealPresence Resource Manager system can provide online/offline status and alerts, display call status, and provide image support including near and far end images for these endpoints.

### Supported Endpoint Types

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Provisioned for selected LifeSize Models?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display 2 Energy Saver</td>
<td>Y</td>
</tr>
<tr>
<td>Display 2 Resolution</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Diagnostics &gt; Cameras</strong></td>
<td></td>
</tr>
<tr>
<td>Camera Anti-Flicker</td>
<td>Y</td>
</tr>
<tr>
<td>HD Camera 1 Brightness</td>
<td>Y</td>
</tr>
<tr>
<td>HD Camera 1 White Balance</td>
<td>Y</td>
</tr>
<tr>
<td>HD Camera 2 White Balance</td>
<td>Y</td>
</tr>
<tr>
<td>HD Camera 2 Brightness</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Diagnostics &gt; DVD-I Input</strong></td>
<td></td>
</tr>
<tr>
<td>DVI-I Input Horizontal Position</td>
<td>Y</td>
</tr>
<tr>
<td>DVI-I Input Vertical Position</td>
<td>Y</td>
</tr>
<tr>
<td>DVI-I Input Coarse Tuning</td>
<td>Y</td>
</tr>
<tr>
<td>DVI-I Input Fine Tuning</td>
<td>Y</td>
</tr>
<tr>
<td>DVI-I Input Brightness</td>
<td>Y</td>
</tr>
<tr>
<td>DVI_I Input Contrast</td>
<td>Y</td>
</tr>
<tr>
<td>DVI-I Input Scaling</td>
<td>Y</td>
</tr>
</tbody>
</table>
Reference for Provisionable Endpoint Fields

Endpoint Fields for Automatic Provisioning

The following table shows the fields you can configure when adding a new automatic provisioning profile to the Polycom® RealPresence® Resource Manager system. You may find more implementation details about these fields in the endpoint system documentation.

To view these fields, go to Admin > Provisioning Profiles > Automatic Provisioning Profiles.

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>Specifies the language for the video endpoint system’s user interface. Possible values include: English, German, Spanish, French, and Chinese (Simplified Chinese only).</td>
</tr>
<tr>
<td>Allow Access to User Setup</td>
<td>Specifies whether the User Settings screen is accessible to users via the System screen. Select this option to allow endpoint system users to change limited environmental settings.</td>
</tr>
<tr>
<td>Allow Directory Changes</td>
<td>Specifies whether endpoint system users can save changes they make to the directory on contacts/favorites list.</td>
</tr>
<tr>
<td>Call Detail Report</td>
<td>Specifies whether to collect call data for the Call Detail Report and Recent Calls list. When selected, information about calls can be viewed through the endpoint system’s web interface and downloaded as a .csv file.</td>
</tr>
</tbody>
</table>

**Note**

If this setting is disabled, applications will not be able to retrieve Call Detail Report (CDR) records.
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Time in Call (minutes)</td>
<td>Specifies the maximum number of minutes allowed for a call. Enter 0 to remove any limit.</td>
</tr>
</tbody>
</table>
| Recent Calls                      | Specifies whether to display the Recent Calls button on the home screen. The Recent Calls screen lists the site number or name, the date and time, and whether the call was incoming or outgoing.  
**Note**  
If the Call Detail Report option is not selected, the Recent Calls option is not available. |
| Screen Saver Wait Time            | Specifies how long the system remains awake during periods of inactivity. The default is 3 minutes. If the system requires users to log in, the screen saver timeout also logs out the current user. Setting this option to Off prevents the system from going to sleep. To prevent image burn-in, specify 15 minutes or less. |
| Directory Search Mode             | Specifies how endpoint directory searches are initiated by the endpoint user. Possible values are:  
• Auto—The search is executed after the user stops entering characters.  
• Manual—The search is executed only when the user explicitly clicks the Search button. |
| Maximum Number of Active Web Sessions | Specifies the number of active web sessions that are allowed. The default is 25. |

**Home Screen Settings**

| Display H.323 Extension            | Lets users placing a gateway call enter the H.323 extension separately from the gateway ID.  
If you do not select this setting, endpoint system users make gateway calls by entering the call information in this format: gateway ID + ## + extension |
| Enable Availability Control       | When enabled, lets users set their availability in the endpoint system's local user interface. |

**H.323 Settings**

| Maximum Speed for Receiving Calls (kbps) | Allows you to restrict the bandwidth used when receiving calls.  
If the far site attempts to call the endpoint system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field. The default is 384 kbps. |
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred Speed for Placing Calls (kbps)</td>
<td>Determines the speeds that will be used for calls from this endpoint system when:</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Call Quality</strong> selection is either unavailable or set to <strong>Auto</strong> on the <strong>Place a Call</strong> screen</td>
</tr>
<tr>
<td></td>
<td>• The call is placed from the directory</td>
</tr>
<tr>
<td></td>
<td>If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.</td>
</tr>
<tr>
<td></td>
<td>The default is <strong>384</strong> kbps.</td>
</tr>
</tbody>
</table>

**Call Settings**

| Preferred Dialing Method                      | Specifies the preferred method for dialing various call types.                                                                                                                                                                               |
|                                               | • If set to **Auto** (default), calls use the configured dialing order.                                                                                                                                                                     |
|                                               | • If set to **Manual**, the endpoint systems will prompt the user to select the call type from a list when placing a call.                                                                                                                     |

**Audio Settings**

| Mute Auto Answer Calls                        | Specifies whether or not to automatically mute incoming calls.                                                                                                                                                                               |
|                                               | The default setting is to **not** automatically mute incoming called.                                                                                                                                                                       |

**CMA Desktop Settings**

| Allow IM/Chat                                  | When enabled, specifies that the Polycom CMA Desktop client can initiate instant messaging. This is enabled by default.                                                                                                                        |
| Enable Screen Saver When in Call              |                                                                                                                                                                                                                                           |
| Provision Check that the CMA Desktop is the default program for: | • Opening Call To links                                                                                                                                                                                                               |
|                                               | • Opening H323 links                                                                                                                                                                                                                      |
|                                               | • Opening SIP links                                                                                                                                                                                                                      |
|                                               | Marking this setting provisions the CMA Desktop to be the default program for opening the above links.                                                                                                                                  |
| Provision Enable Sending 720p (HD) Video      | Mark this check box to enable sending HD video. This is enabled by default.                                                                                                                                                                |
| Allow 720p frame rates up to:                 | Enabled when Provision Enable Sending 720p (HD) people video is also marked. You can choose 15 Frames per second or 30 Frames per second.                                                                                                      |
The following table shows the fields you can configure when adding a new scheduled provisioning profile. You may find more implementation details about these fields in the endpoint system documentation.

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendaring Settings</td>
<td></td>
</tr>
<tr>
<td>Enable Calendaring</td>
<td>When enabled, specifies that the RealPresence Resource Manager system will provision the endpoint for Polycom Conferencing for Outlook. This includes provisioning the Microsoft Exchange server and calendaring settings for the endpoint system.</td>
</tr>
<tr>
<td>Alert Tone</td>
<td>When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will play a sound along with the meeting reminder. In this case, the endpoint will only play a sound when the system is not in a call.</td>
</tr>
<tr>
<td>Display Private Meeting</td>
<td>When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will display details about meetings marked private.</td>
</tr>
<tr>
<td>Meeting Reminder Time</td>
<td>Specifies the number of minutes before the meeting an endpoint system provisioned for Polycom Conferencing for Outlook will display a reminder.</td>
</tr>
<tr>
<td>Microsoft Lync Settings</td>
<td></td>
</tr>
<tr>
<td>Group Name</td>
<td>Specifies the group name for which the endpoint system should be provisioned.</td>
</tr>
<tr>
<td>VVX Settings</td>
<td></td>
</tr>
<tr>
<td>Configuration Server URL</td>
<td>Specifies the IP address for the system that will provide provisioning service. All addresses can be followed by an optional directory and optional filename.</td>
</tr>
<tr>
<td>Logging Server URL</td>
<td>Specifies the directory to use for log files, if required. A URL can also be specified. This field is blank by default.</td>
</tr>
<tr>
<td>Configuration Data</td>
<td>Enter XML data for a custom configuration. Allows the RealPresence Resource Manager system administrator’s to provision settings that the RealPresence Resource Manager system does not normally provide.</td>
</tr>
</tbody>
</table>
To view or create scheduled provisioning profiles, select **Admin > Provisioning Profiles > Scheduled Profiles.**

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings &gt; System Settings &gt; System Settings 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Time in Call (minutes)</td>
<td>Specifies the maximum number of minutes allowed for a call. Enter 0 to remove any limit.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow Mixed IP and ISDN calls</td>
<td>Specifies whether users can make multipoint calls that include both IP and H.320 sites.</td>
<td>Y Y —</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Answer Point-to-Point Calls</td>
<td>Specifies whether to set the endpoint system to answer incoming point-to-point calls automatically.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Answer Multipoint Calls</td>
<td>Specifies whether to set the endpoint system to answer incoming multipoint calls automatically.</td>
<td>Y Y —</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow Directory Changes</td>
<td>Specifies whether users can save changes to the directory or contacts/favorites list.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirm Directory Additions Upon Call Disconnect</td>
<td>Specifies whether users are prompted to confirm deletions of directory entries.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirm Directory Deletions</td>
<td>Specifies whether users are prompted to confirm new directory entries when saving the information for the last site called.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow Access to User Setup</td>
<td>Specifies whether the User Settings screen is accessible to users via the System screen. Select this option to allow users to change limited environmental settings.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>General Settings &gt; System Settings &gt; System Settings 2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Far Site Name Display</td>
<td>Specifies how long the far site name to appear on the screen when the call is first connected.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Time in Call</td>
<td>Displays time that the current call has been connected</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keypad Audio Confirmation</td>
<td>Allows the user to hear a voice confirmation of the numbers selected with the remote control.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Detail Report</td>
<td>Collects call data.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recent Calls</td>
<td>Provides navigational tool for call history.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Color Scheme</td>
<td>Enables the customization of the look of the system with five different color schemes.</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen Saver Wait Time</td>
<td>The time the system will delay before going into standby mode after nonuse</td>
<td>Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems being provisioned...</td>
<td>HDX Series</td>
<td>VSX Series</td>
<td>QDX Series</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>General Settings &gt; Home Screen Settings &gt; Home Screen Settings 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dialing Display</td>
<td>Dialing entry field - Includes the dialing entry field on the Home screen. Display Marquee - Allows the addition of text to the dialing entry field of the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Enter Marquee Text</td>
<td>Enter the Marquee text that will appear in the “Dialing entry field” when Display Marquee is selected.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Call Quality</td>
<td>Allow users to select the speed/bandwidth of the call.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Display H.323 Extension</td>
<td>Displays the IP dialing extension on the main call screen</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Directory</td>
<td>Includes the Directory button on the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>System</td>
<td>Includes the System button on the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Multipoint</td>
<td>Includes the Multipoint navigational item on the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td><strong>General Settings &gt; Home Screen Settings &gt; Home Screen Settings 2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>Enable when the system name is to be displayed on the Home Screen.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>IP or ISDN Information</td>
<td>• Both – Displays both number types on the system’s Home screen. • IP only – Display the system IP number on the Home screen. • ISDN only – Displays the system ISDN number on the Home screen. • None – The system will not display contact numbers on the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Local Date and Time</td>
<td>Displays the local time on the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Enable Availability Control</td>
<td>Displays availability icons on the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Sites</td>
<td>Displays icons created for frequently called sites on the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Last Number Dialed</td>
<td>Displays the last number dialed on the Home screen.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### General Settings > Security

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access Password</td>
<td>Specifies the password for administrator access when logging in to the system remotely. When the remote access password is set, users must enter it to manage the system from a computer. The remote access password must not contain spaces.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Meeting Password</td>
<td>Specifies the password users must supply to join multipoint calls on this system if the call uses the internal multipoint option, rather than a bridge. The meeting password must not contain spaces. Do not set a meeting password if multipoint calls will include audio-only endpoints. Audio-only endpoints cannot participate in password-protected calls.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Enable FTP Access</td>
<td>Specifies that the endpoint system can be accessed via an FTP session. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Enable Web Access</td>
<td>Specifies that the endpoint system can be accessed via its web interface. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Enable Telnet Access</td>
<td>Specifies that the endpoint system can be accessed via a telnet session. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### AES Encryption

Specifies how to encrypt calls with other sites that support AES encryption.
- Off—AES Encryption is disabled.
- When Available—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don’t support it.
- Required for Video Calls Only—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are allowed. Video endpoints must support AES Encryption to participate in the call.
- Required for All Calls—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are not allowed. All endpoints must support AES Encryption to participate in the call.

<table>
<thead>
<tr>
<th>Field</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES Encryption</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

### General Settings > Date and Time 1

<table>
<thead>
<tr>
<th>Field</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Format</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Time Format</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Month</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Day</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Year</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Hour</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Minute</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>AM/PM</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Auto Adjust for Daylight Saving Time</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Time Difference from GMT</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Time Server</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Reference for Provisionable Endpoint Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Time Server Address</td>
<td>Specifies the address of the time server to use when Time Server is set to Manual.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

#### Video Network > IP Network > Call Preferences

| Enable IP H.323               | Allows the system to make IP calls             | Y          | Y          | Y          |
| Enable H.239                  | Specifies standards-based People+Content data collaboration. Enable this option if you know that H.239 is supported by the far sites you will call. If callers experience issues when sharing content with other Polycom systems, disable this setting. | Y          | Y          | Y          |
| Enable Transcoding            | Specifies whether the system allows each far-site system to connect at the best possible call rate and audio/video algorithm. If transcoding is disabled, the Polycom HDX system down-speeds all connections to the same call rate. | Y          | Y          |            |
| ISDN Gateway                  | Allows users to place IP-to-ISDN calls through a gateway. | Y          | Y          | Y          |
| IP Gateway                    | Allows users to place ISDN-to-IP or IP-to-IP calls through a gateway. | Y          | —          |            |

#### Video Network > IP Network > Gatekeeper

| Use Gatekeeper                | Specifies whether to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. • Off — Calls do not use a gatekeeper. • Auto — System attempts to automatically find an available gatekeeper. • Specify — Calls use the specified gatekeeper. Enter the gatekeeper’s IP address or name (for example, gatekeeper.companyname.usa.com, or 10.11.12.13). | Y          | Y          | Y          |
| Gatekeeper IP Address         | If you chose to use an automatically selected gatekeeper, this area displays the gatekeeper’s IP address. If you chose to specify a gatekeeper, enter the IP address. | Y          | Y          | Y          |
| Use Gatekeeper for Multipoint Calls | Specify whether multipoint calls use the system’s internal multipoint capability or the Conference on Demand feature. | Y          | Y          |            |

#### Video Network > IP Network > Gateway Number

| Country Code                  | Specifies the country code for the system’s location | Y          | Y          |            |
| Area Code                    | Specifies the area or city code for the system’s location | Y          | Y          |            |
| Gateway Number               | Specifies the gateway’s number                       | Y          | Y          |            |
### Gateway Number Type
Specifies the number type users enter to call this system:
- **Direct Inward Dial** — Users enter an internal extension to call this system directly.

**Note**
If you choose this setting, you must also register the number with the gatekeeper as an E.164 alias.
- **Number + Extension** — Users enter the gateway number and the system’s extension to call this system.

### Number of digits in DID Number
Specifies the number of digits in the DID number.
The national or regional dialing plan for your location determines the standard number of digits. For instance, the US standard is 7 digits.

### Number of digits in Extension
Specifies the number of digits in the extension used when Direct Inward Dial is selected.
Your organization’s dial plan determines this number.

### Video Network > IP Network > Quality of Service Settings
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Service Field</strong></td>
<td>Specifies the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Precedence</strong> — Represents the priority of IP packets sent to the system. The value can be between 0 and 7.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Diffserv</strong> — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Video Type of Service Value</strong></td>
<td>Specifies the IP Precedence or Diffserv value for video packets. This value does not apply to the CMA Desktop system. It’s value is set by the client’s operating system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Audio Type of Service Value</strong></td>
<td>Specifies the IP Precedence or Diffserv value for audio packets.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FECC Type of Service Value</strong></td>
<td>Specifies the IP Precedence or Diffserv value for Far End Camera Control packets.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Enable Dynamic Bandwidth</strong></td>
<td>Specifies whether to let the system automatically find the optimum line speed for a call</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Enable PVEC</strong></td>
<td>Allows the system to use PVEC (Polycom Video Error Concealment) if packet loss occurs.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Reference for Provisionable Endpoint Fields

#### Video Network > IP Network > Firewall Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Fixed Ports</td>
<td>Specifies whether to define the TCP and UDP ports.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>- If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If the firewall is not H.323 compatible, enable this setting. The endpoint systems will assign a range of ports starting with the TCP and UDP ports you specify. The endpoint system defaults to a range beginning with port 3230 for both TCP and UDP.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must open the corresponding ports in the firewall. You must also open the firewall’s TCP port 1720 to allow H.323 traffic.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start TCP Port</td>
<td>Allows you to specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must also open the firewall’s TCP port 1720 to allow H.323 traffic.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start UDP Port</td>
<td>Allows you to specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>NAT Configuration</td>
<td>Specifies whether the endpoint systems should determine the NAT Public WAN Address automatically.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>- If the endpoint systems are behind a NAT that allows HTTP traffic, select <strong>Auto</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If the endpoint systems are behind a NAT that does not allow HTTP traffic, select <strong>Manual</strong>. Then specify a <strong>NAT Public (WAN) Address</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If the endpoint systems are not behind a NAT or are connected to the IP network through a virtual private network (VPN), select <strong>Off</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT Public (WAN) Address</td>
<td>When <strong>NAT Configuration</strong> is set to Manual, specifies the address that callers from outside the LAN should use to call the endpoint systems.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>NAT is H.323 Compatible</td>
<td>Specifies that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems being provisioned...</td>
<td>HDX Series</td>
<td>VSX Series</td>
<td>QDX Series</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>Address Displayed in Global Directory</td>
<td>Specifies whether or not to include the endpoint system's information in the global directory</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Video Network &gt; ISDN BRI Protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable ISDN H.320</td>
<td>Allows this system to make H.320 (ISDN) calls.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Number of ISDN Channels to Dial in Parallel</td>
<td>Specifies how many channels to dial at one time. You can specify up to eight channels. If you experience network problems, decrease the number. Set this value to 1 for serial dialing. Serial dialing is not recommended unless you have trouble connecting calls using parallel dialing.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>ISDN Switch Protocols</td>
<td>Specifies the protocol used by your network's switch.</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Outside Line Dialing Prefix</td>
<td>Specifies the ISDN dialing prefix used to call outside the network.</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Video Network &gt; Preferred Speeds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preferred Speed for Placing Calls (Kbps)</td>
<td>Determines the speeds that will be used for IP, ISDN, or International ISDN calls from this endpoint system when:</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>IP Calls</td>
<td>• The Call Quality selection is either unavailable or set to Auto on the Place a Call screen</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN Video Call (H.320)</td>
<td>• The call is placed from the directory If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>International ISDN calls</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Maximum Speed for Receiving Calls (Kbps)</td>
<td>Allows you to restrict the bandwidth used when receiving IP or ISDN calls.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>IP Calls</td>
<td>If the far site attempts to call the system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>ISDN Video Call (H.320)</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Monitors &gt; Monitors 1</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Number of Monitors</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Monitor 1 Options</td>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Monitor 1</td>
<td>Specifies the monitor's aspect ratio. • 4:3 — Select if you are using a regular TV monitor.</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems being provisioned...</td>
<td>HDX Series</td>
<td>VSX Series</td>
<td>QDX Series</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>Video Format</td>
<td>Specifies the monitor’s format:</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DVI — Select if the monitor is connected to the DVI connector using a DVI or HDMI cable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VGA — Select if the monitor is connected to the DVI connector using a VGA cable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Component YPbPr — Select if the monitor is connected to the DVI connector using component cables. Polycom HDX 8000 series and Polycom HDX 7000 series systems do not support 720p Component format for 50 Hz monitors.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• S-Video (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using an S-Video cable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Composite (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using a composite video cable.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Icons in Call</td>
<td>Specifies whether to display all on-screen graphics, including icons and help text, during calls.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Snapshot Timeout</td>
<td>Lets you choose whether to have slides and snapshots time out after a period of four minutes.</td>
<td>—</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Dual Monitor Emulation</td>
<td>Specifies whether the system can show multiple views on a single display.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Output Upon Screen Saver Activation</td>
<td>Specifies whether black video or no signal is sent to the monitor when the system goes to sleep and the screen saver activates.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Black</strong> to display black video. This is the recommended setting to prevent burn-in for TV monitors.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Select <strong>No Signal</strong> to have the display react as if it is not connected when the system goes to sleep. This is the recommended setting for VGA monitors and projectors.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VGA Resolution</td>
<td></td>
<td>—</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Monitor 2 Options</td>
<td><strong>Applies to:</strong></td>
<td>Y</td>
<td>—</td>
<td>Y</td>
</tr>
<tr>
<td>Monitor 2</td>
<td>Specifies the second monitor’s aspect ratio:</td>
<td>Y</td>
<td>—</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>• Off — Select if you do not have a second monitor.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4:3 — Select if you are using a regular TV monitor as the second monitor.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems being provisioned...</td>
<td>HDX Series</td>
<td>VSX Series</td>
<td>QDX Series</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>Video Format</td>
<td>Specifies the monitor’s format:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DVI — Select if the monitor is</td>
<td></td>
<td>Y</td>
<td>—</td>
<td>Y</td>
</tr>
<tr>
<td>connected to the DVI connector</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>using a DVI or HDMI cable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• VGA — Select if the monitor is</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connected to the DVI connector</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>using a VGA cable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Component YPbPr — Select if the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>monitor is connected to the DVI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connector using component cables.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom HDX 8000 series and Polycom</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDX 7000 series systems do not</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>support 720p Component format for</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50 Hz monitors.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S-Video (Polycom HDX 9000 series</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>only) — Select if the monitor is</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connected to the BNC connectors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>using an S-Video cable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Composite (Polycom HDX 9000 series</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>only) — Select if the monitor is</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connected to the BNC connectors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>using a composite video cable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output Upon Screen Saver Activation</td>
<td>Specifies whether black video or no signal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specified on the monitor when</td>
<td>is sent to the monitor when the system goes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to sleep and the screen saver</td>
<td>to sleep and the screen saver activates.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Select <strong>Black</strong> to display black</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>video. This is the recommended</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>setting to prevent burn-in for TV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>monitors.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Select <strong>No Signal</strong> to have the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>display react as if it is not</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>connected when the system goes to</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sleep. This is the recommended</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>setting for VGA monitors and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>projectors.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>People Display Mode</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Display Mode</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Color System</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Monitor 3 Options</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor 3</td>
<td>Specifies the aspect ratio for recording.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Off — Select if you do not have</td>
<td></td>
<td>Y</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>a VCR or DVD player connected to</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>record video conferences.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 4:3 — Select to record for</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>playback on a standard monitor.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 16:9—Select to record for</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>playback on a wide-screen monitor,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>if your recording device has this</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>capability.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>See the endpoint product</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>documentation for more information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>about these selections.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems being provisioned...</td>
<td>HDX Series</td>
<td>VSX Series</td>
<td>QDX Series</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
| Video Format                  | Specifies the VCR or DVD player's format:  
• S-Video — Select if the VCR or DVD player is connected to a Polycom HDX system using an S-Video cable.  
• Composite — Select if the VCR or DVD player is connected to a Polycom HDX system using a composite video cable and S-Video to RCA adapter.                                                                                                 | Y          | —          |            |
| Output Upon Screen Saver Activation | Specifies whether black video or no signal is sent to the VCR or DVD player when the system goes to sleep and the screen saver activates.  
• Select Black to send black video.  
• Select No Signal to have the VCR or DVD player react as if it is not connected when the system goes to sleep.                                                                 | Y          | —          |            |
| VCR/DVD Record Source         | Specifies the video source to be recorded to videotape or DVD.                                                                                                                                                                                                                                           | Y          | —          |            |
| Near                          | If Far is enabled, the recorded video will switch to the current far site speaker.                                                                                                                                                                                                                           | Y          | —          |            |
| Far                           | If both Near and Far are enabled, the recorded video will switch between near and far sites depending on the current speaker.                                                                                                                                                                                  | Y          | —          |            |
| Content                       | If Content is enabled, any content sent during the call is recorded.                                                                                                                                                                                                                                         | Y          | —          |            |
| Screen Saver Wait Time        | The time the system will delay before going into standby mode after nonuse                                                                                                                                                                                                                                  | Y          | —          |            |
| Cameras > Cameras 1           |                                                                                                                                                                                                                                                                                                               |            |            |            |
| Far Control of Near Camera    | Specifies whether the far site can pan, tilt, or zoom the near-site camera. When this option is selected, a user at the far site can control the framing and angle of the camera for the best view of the near site.                                                                                                                      | Y          | Y          | Y          |
| Backlight Compensation        | Specifies whether the camera should automatically adjust for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background.                                                                                                                        | Y          | Y          | Y          |
| Primary Camera                | Specifies which camera is the main camera.                                                                                                                                                                                                                                                                    | Y          | Y          | Y          |
| Camera Direction              | Specifies the direction the camera moves when using the arrow buttons on the remote control.                                                                                                                                                                                                                 | Y          | Y          | Y          |
| Cameras > Camera Settings     |                                                                                                                                                                                                                                                                                                               |            |            |            |
| Camera 1 Name                 | Specifies a name for camera 1.                                                                                                                                                                                                                                                                         | Y          | Y          | Y          |
### Field | For the endpoint systems being provisioned... | HDX Series | VSX Series | QDX Series
--- | --- | --- | --- | ---
Camera 1 Icon | Specifies an icon for camera 1. | Y | Y | Y
Camera 2 Name | Specifies a name for camera 2. | Y | Y | Y
Camera 2 Icon | Specifies an icon for camera 2. | Y | Y | Y
Camera 3 Name | Specifies a name for camera 3. | Y | Y | Y
Camera 3 Icon | Specifies an icon for camera 3. | Y | Y | Y

### Cameras > Video Quality

<table>
<thead>
<tr>
<th>Camera</th>
<th>Specifies Motion or Sharpness for the video input. The default is Sharpness.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera 1</td>
<td><strong>Motion</strong> — This setting is for showing people or other video with motion.</td>
</tr>
<tr>
<td>Camera 2</td>
<td><strong>Sharpness</strong> — The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped. Sharpness is available in point-to-point H.263 and H.264 calls only. It is recommended for HD calls between 1 Mbps and 2 Mbps.</td>
</tr>
</tbody>
</table>

### Audio Settings > Audio Settings 1

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
</table>
| Sound Effects Volume | Sets the volume level of the ring tone and user alert tones. | Y | Y | Y
| Incoming Video Call | Specifies the ring tone used for incoming calls. | Y | Y | Y
| User Alert Tones | Specifies the tone used for user alerts. | Y | Y | Y
| Mute Auto Answer Calls | Specifies whether to mute incoming calls. |
| | Incoming calls are muted by default until you press the mute on the microphone or on the remote control. | Y | Y | Y
| Line Input | Specifies the type of equipment that is connected to audio input 1. | Y | Y |
| Input Type Level | Sets the volume level for audio input 1. | Y | Y |
| Line Input Level | Sets the volume level for audio input 2. | Y | Y |
| Line Outputs | Specifies how the audio output behaves. The default selection, **Monitor - Far Site Audio**, supplies audio to the Monitor 1 audio outputs only when the system is receiving audio from the far site. If you have connected a VCR to record the conference, select **Monitor - Far and Near Audio** to supply audio from both the far site and the system’s microphones. | Y | Y |
### Audio Settings > Audio Settings 2

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Output Level</td>
<td>Sets the volume level for audio output</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Master Audio Volume</td>
<td>Sets the volume level for audio from the far site.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Midrange Speakers</td>
<td>Specifies whether to use the system's built-in midrange speaker. You may prefer to turn off the midrange speaker if you connect the audio output to Monitor 1 or if you connect an external speaker system.</td>
<td>—</td>
<td>Y</td>
<td>—</td>
</tr>
<tr>
<td>Bass</td>
<td>Sets the volume level for the low frequencies without changing the master audio volume.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Treble</td>
<td>Sets the volume level for the high frequencies without changing the master audio volume.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### LAN Properties > LAN Properties 1

<table>
<thead>
<tr>
<th>Field</th>
<th>Enables connection to the local area network</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to My LAN</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies how the system obtains an IP address.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Obtain IP Address Automatically — Select if the system gets an IP address from the DHCP server on the LAN.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>• Enter IP Address Manually — Select if the IP address will not be assigned automatically.</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Use the Following IP Address</td>
<td>If you selected Enter IP Address Manually, enter the IP address here.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### LAN Properties > LAN Properties 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Displays the DNS servers currently assigned to the system.</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Servers</td>
<td>If the system does not automatically obtain a DNS server address, enter up to four DNS servers here. Changing this setting causes the system to restart.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here. Changing this setting causes the system to restart.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here. Changing this setting causes the system to restart.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned…</th>
</tr>
</thead>
<tbody>
<tr>
<td>WINS Server</td>
<td>Displays the server running the Windows Internet Name Service</td>
</tr>
<tr>
<td>WINS Resolution</td>
<td>Enables connection to the WINS Server for URL resolution</td>
</tr>
<tr>
<td>LAN Speed</td>
<td>Specify the LAN speed to use. Note that the setting you choose must be supported by the switch. Choose Auto to have the network switch negotiate the speed automatically. In this case, the switch must also be set to Auto. Choosing Auto automatically sets Duplex Mode to Auto. If you choose 10 Mbps, 100 Mbps, or 1000 Mbps you must set Duplex Mode to Half or Full. Changing this setting causes the system to restart.<strong>Note</strong> Mismatches with the network switch settings may lead to unexpected behaviors. <strong>Y</strong> <strong>Y</strong> <strong>Y</strong></td>
</tr>
<tr>
<td>Duplex Mode</td>
<td>Specify the duplex mode to use. Note that the Duplex mode you choose must be supported by the switch. Choose Auto to have the network switch negotiate the Duplex mode automatically. In this case, the switch must also be set to Auto. Choosing Auto automatically sets LAN Speed to Auto. Changing this setting causes the system to restart. <strong>Y</strong> <strong>Y</strong> <strong>Y</strong></td>
</tr>
</tbody>
</table>

### Global Services > Directory Servers

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Directory (GDS)</td>
<td>Specifies the IP address or DNS address of the Global Directory Server.</td>
</tr>
<tr>
<td>Password</td>
<td>Lets you enter the global directory password, if there is one.</td>
</tr>
<tr>
<td>Display Name in Global Directory</td>
<td>Specifies whether to display the system’s name in the global directories of other registered systems. Global Address</td>
</tr>
<tr>
<td>Display Global Addresses</td>
<td>Displays other registered systems in the global directory.</td>
</tr>
<tr>
<td>Register</td>
<td>Registers this system with the Global Directory Server.</td>
</tr>
</tbody>
</table>
### Reference for Provisionable Endpoint Fields

#### LAN/H.323 > Global Directory (GDS) > Preferences

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save Global Directory to System</td>
<td>Copies the global directory to this local system. When this setting is disabled, the system can display no more than 1,000 global directory entries. When this setting is enabled, the system can display up to 4,000 global directory entries.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Show Addresses in Address Book</td>
<td></td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Preferred Speed for Placing Calls (Kbps)</td>
<td>Determines the speeds that will be used for IP, ISDN, or International ISDN calls from this endpoint system when:</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>ISDN Video Call (H.320)</td>
<td>• The Call Quality selection is either unavailable or set to Auto on the Place a Call screen</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>International ISDN calls</td>
<td>• The call is placed from the directory</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>IP Calls</td>
<td>If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

#### LAN/H.323 > Global Directory (GDS) > Preferred Alias

<table>
<thead>
<tr>
<th>Field</th>
<th>Possible values include:</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred Alias</td>
<td>Gateway Number</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>ISDN Number</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Called Party Line Identifier</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Extension</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

#### Global Services > Account Validation

<table>
<thead>
<tr>
<th>Field</th>
<th>Specify whether to require an account number for placing calls and whether that number should be validated by the system.</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Account Number to Dial</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Validate Account Number</td>
<td>Specify whether to require an account number for placing calls and whether that number should be validated by the system.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

#### Global Services > My Info

<table>
<thead>
<tr>
<th>Field</th>
<th>Specifies the name of the person responsible for this system</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Person</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Contact Number</td>
<td>Specifies the phone number of the person responsible for this system</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Contact Email</td>
<td>Specifies the email address of the person responsible for this system</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems being provisioned...</td>
<td>HDX Series</td>
<td>VSX Series</td>
<td>QDX Series</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>Contact Fax</td>
<td>Specifies the Fax number of the person responsible for this system</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Tech Support</td>
<td>Specifies the contact information for Technical Support for this system</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>City</td>
<td>Specifies the location of the person responsible for this system</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>State/Province</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Country</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
Endpoint Device Details

This chapter identifies the fields found in the Device Detail section of the Polycom® RealPresence® Resource Manager system interface. It includes these topics:

- “Endpoint Device Summary Information” on page 213
- “Device Status Information” on page 216
- “Call Information” on page 218
- “Device Alerts Information” on page 219
- “Provisioning Details” on page 219
- “Software Update Details” on page 220

Endpoint Device Summary Information

The Device Summary information for endpoints in the Monitor View section includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of device. For valid device types, see “Supported Endpoint Types” on page 161.</td>
</tr>
<tr>
<td>ID</td>
<td>The system-generated ID for the device.</td>
</tr>
<tr>
<td>Owner</td>
<td>(Endpoints only) The user associated with the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The assigned IP address of the device.</td>
</tr>
<tr>
<td>Area</td>
<td>Area with which the device is associated. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ISDN Video Number</td>
<td>For ISDN devices only, the country code + city/area code + phone number for the device. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The Resource Manager system only supports native ISDN.</td>
</tr>
<tr>
<td>Site</td>
<td>The network site for the device. By default, devices are added to the <strong>Primary Site</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When areas are enabled on your system, this field shows a value of <strong>Restricted</strong> if you do not have permission to manage the area to which the site is assigned.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number (ASCII only) of the device. The device provides the serial number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Available to Schedule</td>
<td>Select this option to make the device available when users are scheduling conferences.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <strong>Available to schedule</strong> field is disabled for RMX devices.</td>
</tr>
<tr>
<td>Monitoring Level</td>
<td>The monitoring level for the device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Standard</strong>. This device is monitored.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VIP</strong>. This device is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.</td>
</tr>
</tbody>
</table>
Supported Protocols

The communications protocols that the device can support. Possible values include:
- **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP.
- **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.
- **SIP** - A standard that defines the protocols used for multimedia communications over IP.
- For devices with the type **Unknown**, select **H.323**. The device automatically provides the protocols if it registered successfully or is managed.

**Notes**
- If an endpoint is configured as a gateway (ISDN), only the **H.323** check box is selected. If the endpoint supports true ISDN, the **H.323** and **ISDN** check boxes are selected.
- RMX MCUs support only the **H.323** protocol.

Capabilities Enabled

Capabilities to enable on this device. Options are:
- **MCU** - The device can act as a control unit for multipoint conferences
- **Gateway** - The device can act as a gateway for call management

The MCU provides the capability if it registered successfully or is managed.

**Note**
Currently, RMX MCUs cannot be Gateway devices.
Device Status Information

The Device Status information in the Device Details section includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Gatekeeper Registration | The status of the device’s registration with the gatekeeper service. Possible values include:  
  • Registered  
  • Unregistered |
| Directory Registration | The status of the device’s registration with the Global Directory Service. Possible values include:  
  • Registered  
  • Unregistered |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence Registration</td>
<td>The status of the device’s registration with the presence service. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Registered</td>
</tr>
<tr>
<td></td>
<td>• Unregistered</td>
</tr>
<tr>
<td>Exchange Registration</td>
<td>The status of the device’s registration with the Microsoft Exchange service.</td>
</tr>
<tr>
<td>SIP Registration</td>
<td>The status of the device’s registration with the SIP service.</td>
</tr>
<tr>
<td>Device Managed</td>
<td>Indicates whether or not the Resource Manager system is managing the device.</td>
</tr>
<tr>
<td>Gatekeeper Address</td>
<td>The IP address of the gatekeeper to which the device is registered.</td>
</tr>
<tr>
<td>Device Local Time</td>
<td>The local time as set within the device in a default format of hh:mm:ss AM</td>
</tr>
<tr>
<td>ISDN Line Status Type</td>
<td>The status of the ISDN line. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Operational ❇️</td>
</tr>
<tr>
<td></td>
<td>• Non-operations ❇️</td>
</tr>
<tr>
<td></td>
<td>This field is blank for the following device types: <strong>RMX</strong>, <strong>GW/MCU</strong>, <strong>Other</strong>, and <strong>TANDBERG</strong>.</td>
</tr>
<tr>
<td>ISDN Assignment Type</td>
<td>How the ISDN type was assigned to the device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Administrator, when the ISDN type was assigned manually by an administrator</td>
</tr>
<tr>
<td></td>
<td>• Endpoint, when the ISDN type was natively assigned in the endpoint</td>
</tr>
<tr>
<td></td>
<td>• Auto-Assigned, when the ISDN type was automatically assigned by the Resource Manager system based on the site configuration</td>
</tr>
<tr>
<td></td>
<td>• From Network, when the ISDN type was derived from the gateway and extension</td>
</tr>
<tr>
<td></td>
<td>• Undefined, when the Resource Manager system cannot identify the source for the ISDN type assignment</td>
</tr>
<tr>
<td></td>
<td>This field is blank for the following device types: <strong>RMX</strong>, <strong>GW/MCU</strong>, <strong>Other</strong>, and <strong>TANDBERG</strong>.</td>
</tr>
<tr>
<td>Device ISDN Type</td>
<td>The ISDN network interface type installed in the device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• ISDN_QUAD_BRI</td>
</tr>
<tr>
<td></td>
<td>• ISDN_PRI_T1</td>
</tr>
<tr>
<td></td>
<td>• ISDN_BRI</td>
</tr>
<tr>
<td></td>
<td>• ISDN_UNKNOWN</td>
</tr>
<tr>
<td></td>
<td>This field is blank for the following device types: <strong>RMX</strong>, <strong>GW/MCU</strong>, <strong>Other</strong>, and <strong>TANDBERG</strong>.</td>
</tr>
</tbody>
</table>
The **Call Info** in the **Device Details** section includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Type</td>
<td>The connection protocol for the call in which the device is participating. Possible values include: H.323, H.320, and SIP.</td>
</tr>
</tbody>
</table>
| Video Protocol | The video connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include:  
  - H.261  
    H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions.  
  - H.263  
    H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions.  
  - H.264 |
| Video Format   | The video format, both transmission (Tx) and reception (Rx), the device is using. |
| Audio Protocol | The audio connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include:  
  - G.711  
  - G.722  
  - G.728 |
| Far Site Name  | The H.323ID of the far site device to which the selected endpoint is connected. When multiple endpoints are connected through the device's embedded MCU, this field displays a concatenation of each endpoint's H.323ID separated by ' | ', for example 'ISDN-CO1-7-1 | Vsfx-9-1'. |
| Far Site Number| The address of the far site device to which the selected endpoint is connected. The address value for the calling device appears to be the dialed address. The address value for the called device appears to be the IP Address. |
| Cause Code     | Standard H.323 cause code that reflects normal call termination or the nature of an internal failure, for example, '16' or '211'. |
| Encryption     | The status of encryption for the call. Possible values include: Off, Disabled, AES, and DH-1024 |
**Device Alerts Information**

The **Device Alerts** information in the **Device Details** section includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>Device error message text, for example, GK Registration error</td>
</tr>
<tr>
<td>Warnings</td>
<td>Device warning message text, for example, Low Battery</td>
</tr>
</tbody>
</table>

**Provisioning Details**

The **Provisioning Details** information in the **Device Details** section includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Profile Applied</td>
<td>The name of the last provisioning profile that was or was not successfully applied to the device. The <strong>Provisioning Status</strong> will be either <strong>Success</strong> or <strong>Failed</strong>.</td>
</tr>
</tbody>
</table>
| Provisioning Status    | The device’s current provisioning status. Possible values include:  
  - **Clear**. No provisioning has been done.  
  - **Pending**. Provisioning is scheduled for this device.  
  - **In Progress**. The device is currently being provisioned.  
  - **Success**. Provisioning has been completed successfully on this device.  
  - **Failed**. Provisioning was not completed on this device.  
  Some endpoint systems expect all configuration fields to be provisioned. If any of the fields are not provisioned, the status will indicate failed. However, the endpoint will often function successfully. |
| Pending Profile        | The name of the provisioning profile that is scheduled to be applied to the device. In this case, the **Provisioning Status** will be either **Pending** or **In Progress**.  
  This field is blank if the device is not scheduled for provisioning. |
| Scheduled              | The date and time, in the default format of yyyy-mm-dd hh:mm, when the device is schedule to be provisioned.  
  This field is blank if the device is not scheduled for provisioning. |
Software Update Details

The **Software Update Details** information in the **Device Details** section includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Attempt Date/Time</td>
<td>The date and time, in the default format of <code>yyyy-mm-dd hh:mm:ss</code>, of the last provisioning message exchanged with the device.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>A text description of the reason the provisioning failed. Causes for failure include:</td>
</tr>
<tr>
<td></td>
<td>• The provisioning profile does not exist</td>
</tr>
<tr>
<td></td>
<td>• The provisioning profile does not include provisioning information</td>
</tr>
<tr>
<td></td>
<td>• The Resource Manager system no longer manages the device</td>
</tr>
<tr>
<td></td>
<td>• A password for the device is set in the video endpoint system, and you must enter it in the Resource Manager system</td>
</tr>
<tr>
<td></td>
<td>• The device is busy</td>
</tr>
<tr>
<td></td>
<td>• A network error occurred</td>
</tr>
<tr>
<td></td>
<td>• An incomplete transfer of provisioning information occurred</td>
</tr>
<tr>
<td></td>
<td>• Provisioning has timed out</td>
</tr>
<tr>
<td></td>
<td>• An internal error occurred on the device, and you must reboot it</td>
</tr>
<tr>
<td></td>
<td>• An unknown error occurred. Reboot the device.</td>
</tr>
<tr>
<td>Log Message</td>
<td>A read-only text box that contains messages related to the device provisioning status</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Update Status</td>
<td>The device’s software update status. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Clear. A software update has not been done.</td>
</tr>
<tr>
<td></td>
<td>• Pending. A software update has been scheduled and is pending. The device may be offline or in a call.</td>
</tr>
<tr>
<td></td>
<td>• In Progress. The software update is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Success. A software update has completed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Failed. A software update could not be performed.</td>
</tr>
</tbody>
</table>
### Endpoint Device Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduled</strong></td>
<td>The date and time, in the default format of <code>yyyy-mm-dd hh:mm</code>, when the device software is scheduled to be updated. This field is blank if the device is not scheduled for provisioning.</td>
</tr>
<tr>
<td><strong>Last Attempt Date/Time</strong></td>
<td>The date and time, in the default format of <code>yyyy-mm-dd hh:mm:ss</code>, of the last software update message exchanged with the device.</td>
</tr>
<tr>
<td><strong>Failure Reason</strong></td>
<td>A text description of the reason the software update failed. Causes for failure may include:</td>
</tr>
<tr>
<td></td>
<td>• The software update file location does not exist.</td>
</tr>
<tr>
<td></td>
<td>• A password for the device is set in the video endpoint system, and you must enter it in Resource Manager.</td>
</tr>
<tr>
<td></td>
<td>• A network error has occurred.</td>
</tr>
<tr>
<td></td>
<td>• The update has timed out.</td>
</tr>
<tr>
<td></td>
<td>• An internal error occurred on the device, and you must reboot it.</td>
</tr>
<tr>
<td></td>
<td>• A profile has not been configured.</td>
</tr>
<tr>
<td></td>
<td>• An endpoint is offline.</td>
</tr>
<tr>
<td></td>
<td>• An incorrect activation key is in the key file.</td>
</tr>
<tr>
<td></td>
<td>• An unknown error has occurred. Reboot the device.</td>
</tr>
<tr>
<td><strong>Log Message</strong></td>
<td>A read-only text box that contains the log message text recorded during the execution of the software update. Note that there are no log messages displayed for dynamically-managed endpoints.</td>
</tr>
</tbody>
</table>
Understanding Network Device Management

This chapter provides an overview of the Polycom® RealPresence® Resource Manager® system’s network device management functions. This chapter includes these topics:

- Overview of Network Devices
- Monitoring Network Devices

Network devices include any non-endpoint device that the RealPresence Resource Manager system manages or is aware of.

You must have the Device Administrator role to add new network devices to the system or edit their properties. If your system supports multi-tenancy and areas have been enabled, users with the Area Administrator role can also perform some device management tasks.

The remaining user roles can view network devices, but not add new ones or modify settings.

Overview of Network Devices

The RealPresence Resource Manager system supports these network device types:

- MCUs — See “Managing MCU Bridges” on page 229
- Polycom DMA™ system — See “Managing a DMA System” on page 249
- DMA Pool Orders — “Managing DMA Pool Orders” on page 254
- Polycom VBPs — See “Managing Border Controllers and Firewalls” on page 257
- SBCs (session border controls) — See “Managing Border Controllers and Firewalls” on page 257
Monitoring Network Devices

Use the Network Device > Monitor View to monitor the network devices.

- **Monitor View** — Displays the list of all manageable and registered network devices. Use this view to manage network devices.
- **VBPs** (Video Border Proxy systems) — Displays the list of Polycom VBP systems registered to the Resource Manager system. Use this view to add, edit, or delete VBP systems.
- **SBCs** (Session Border Control systems) — Displays the list of SBC systems registered to the Resource Manager system. Use this view to add, edit, or delete SBC systems.
- **MCUs** (Microprocessing Control Units) — Displays the list of Polycom MCUs (Polycom RMX systems) registered to the Resource Manager system. Use this view to add, edit, or delete MCUs.
- **DMA** — Displays the Polycom DMA system registered to the Resource Manager system. Use this view to add, edit, or delete a DMA system.
- **DMA Pool Orders** — Displays the list of Polycom DMA Pool Orders associated with the DMA system that is registered to the Resource Manager system. Use this view to view and edit DMA pool orders.
- **RPADs** — This menu option is reserved for future functionality.

The Network Device > Monitor View has the following information:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Views</td>
<td>The views you can access from the page.</td>
</tr>
<tr>
<td>Actions</td>
<td>The set of available commands. The constant command in the Network Device views is Refresh, which updates the display with current information.</td>
</tr>
<tr>
<td>Network Device List</td>
<td>The context-sensitive Network Device list for the selected view.</td>
</tr>
<tr>
<td>Device Summary</td>
<td>Information about the network device selected in the network device list.</td>
</tr>
</tbody>
</table>
Monitor View

By default the Network Device list in the Monitor View displays a list of all network devices the RealPresence Resource Manager system monitors, including those devices that registered automatically with the system and those devices that were added manually for management and monitoring purposes.

Considerations for Multi-Tenancy

Users with area roles will see only those network devices assigned to the area they manage.

The Network Device list has these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Use the filter choices to display other views of the Network Device list, which include:</td>
</tr>
<tr>
<td></td>
<td>- Type - Filters the list by device type. For more information.</td>
</tr>
<tr>
<td></td>
<td>- Alerts - Filters the list by alert type: Help, Error, or Warning</td>
</tr>
<tr>
<td></td>
<td>- Connection Status - Filters the list by connection status: In a Call, Online, or Offline</td>
</tr>
<tr>
<td></td>
<td>- Name - Filters the list by system name entered</td>
</tr>
<tr>
<td></td>
<td>- IP Address - Filters the list by IP address entered</td>
</tr>
<tr>
<td></td>
<td>- Alias - Filters the list by the alias entered</td>
</tr>
<tr>
<td></td>
<td>- Site - Filters the list by site location entered</td>
</tr>
<tr>
<td></td>
<td>- Area not same as Site's Area - Available only when Areas are enabled.</td>
</tr>
<tr>
<td></td>
<td>This allows you to filter on devices that may have been added to a different area than their site's area. A device and the site it belongs to must be assigned the same area. This filter allows you to troubleshoot any misplaced devices.</td>
</tr>
<tr>
<td></td>
<td>- Area - Available only when Areas are enabled. Filters the list by the area with which the device is associated. You can only view area-specific information for area(s) that you have permission to manage.</td>
</tr>
<tr>
<td>Status</td>
<td>The state of the network device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>- Online</td>
</tr>
<tr>
<td></td>
<td>- Offline</td>
</tr>
<tr>
<td></td>
<td>- In a call</td>
</tr>
<tr>
<td></td>
<td>- Unknown</td>
</tr>
<tr>
<td></td>
<td>- Device alert</td>
</tr>
<tr>
<td></td>
<td>- Gatekeeper not applicable</td>
</tr>
</tbody>
</table>
### Actions in the Monitor View

Besides providing access to the network device views, the Actions section of the Monitor View may also include these context-sensitive commands depending on the selected device type.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The system name of the network device</td>
</tr>
<tr>
<td>Type</td>
<td>The type of network device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the network device</td>
</tr>
<tr>
<td>Site</td>
<td>The site to which the network device belongs.</td>
</tr>
<tr>
<td>Note</td>
<td>When areas are enabled on your system, this field shows a value of <strong>Restricted</strong> if you do not have permission to manage the area to which the site is assigned.</td>
</tr>
<tr>
<td>Area</td>
<td>Available only when <strong>Areas</strong> are enabled. The area with which the network device is associated. Users can only view area information for the areas they have been assigned to manage.</td>
</tr>
</tbody>
</table>

**Actions in the Monitor View**

Available for all device types

- **Add**
  Manually add a network device to the Resource Manager system or find a network device on the network. You can search for using DNS or IP address.

- **Edit**
  Change connection settings for the selected network device. Note that if this is a managed device, the device may overwrite settings entered manually.

- **Delete**
  Delete the selected network devices

- **View Details**
  Display all of the **Device Details** for the selected network device

Available for only selected network device types

- **Manage**
  Open the selected network device’s management interface in a separate browser window.
### Associate Area

Available only for DMA Pool Orders and when **Areas** are enabled.

Associate the selected DMA Pool Order to an area so that only specified area users can use it to schedule conferences.

Users can only view area information for the areas to which they have been assigned to manage.

Only DMA Pool Orders can be associated with an area via this menu. You can associate an RMX system with an area using the Edit option. Other network devices cannot be associated with an area.
This chapter describes how to perform the Polycom® RealPresence® Resource Manager system MCU bridge management tasks. It includes these topics:

- “View Device Details” on page 229
- “Add an MCU Manually” on page 233
- “Edit an MCU Bridge” on page 235
- “Delete an MCU Bridge” on page 238
- “View Bridge Hardware” on page 238
- “View Bridge Services” on page 239
- “View Bridge Conferences” on page 239
- “View Bridge Ports” on page 240
- “View Bridge Meeting Rooms” on page 240
- “View Bridge Entry Queues” on page 241
- “View Bridge Gateway Conferences” on page 241

**MCU View**

Use the **MCU View** to manage Polycom MCU conferencing platforms on the network.

The MCU View allows you to view more detailed information about the MCUs that your system manages.

**View Device Details**

To view detailed information about a managed MCU bridge

1. Go to Network Device > MCUs.
2 As needed, use the **Filter** to customize the MCU list.

3 Select the MCU of interest and click **View Details**.

The **Device Details** dialog box for the selected MCU appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>The name of the MCU.</td>
</tr>
<tr>
<td>System Name</td>
<td>The name of the MCU.</td>
</tr>
<tr>
<td></td>
<td>• MCU names must be unique.</td>
</tr>
<tr>
<td></td>
<td>• If your system integrates with a Polycom DMA system, make sure your MCU system name includes a qualifier that indicates to the DMA system administrator that the MCU is directly registered to the RealPresence Resource Manager; for example, <em>ResourceManager_RMX10</em>.</td>
</tr>
<tr>
<td></td>
<td>• The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid.</td>
</tr>
<tr>
<td></td>
<td>• When retrieved from the MCU, the name is taken from the H.323 ID if the MCU registered with the gatekeeper and it is a third-party system. In other cases, it is the system name, which might be different than the H.323 ID.</td>
</tr>
<tr>
<td>DNS Name</td>
<td>The DNS name of the MCU.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of MCU.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The assigned IP address of the MCU</td>
</tr>
<tr>
<td>Site</td>
<td>The network site for the MCU. By default, MCUs are added to the <strong>Primary Site</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>A free-form text field (Extended ASCII only) in which information about the MCU can be added.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number (ASCII only) of the MCU. The MCU provides the serial number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version of the software installed on the MCU (ASCII only). The MCU provides the version number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTP URL</td>
<td>(Polycom RMX systems only)                                                                                                           The management URL for the endpoint, if available (ASCII only). This URL allows the Resource Manager system to start the endpoint’s management system using the <strong>Manage</strong> function. All Polycom endpoints allow device management through a browser. For these endpoints, this field is completed when the endpoint registers with the Resource Manager system. For third-party endpoints that do not register using an IP address, you must enter the URL.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>(Polycom RMX systems only)                                                                                                           The HTTP port number for the MCU communications. The MCU provides the port number if it registered successfully and is managed. By default, in non-secure (HTTP) mode, the RealPresence Collaboration Server uses port 80 and in secure (HTTPS) mode, the RealPresence Collaboration Server uses port 443.</td>
</tr>
<tr>
<td>Area</td>
<td>This field indicates the area in which the MCU resides.                                                                                                                                                  This field is only visible when Areas are enabled and the user manages more than one area. A user can only view area-specific information for an area(s) that he has permission to manage.</td>
</tr>
<tr>
<td>ISDN Video Number</td>
<td>The country code + city/area code for the MCU.                                                                                                                                                         The main number is automatically read from the ISDN service on the bridge.</td>
</tr>
<tr>
<td>Capabilities</td>
<td>The communications protocols that the MCU can support. Possible values include:                                                                                                                        The MCU automatically provides the protocols if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>• <strong>IP (H.323)</strong> - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ISDN (H.320)</strong> - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP (SIP)</strong> - A standard that defines the protocols used for multimedia communications on SIP networks.</td>
</tr>
</tbody>
</table>
### Capabilities Enabled

Capabilities to enable on this MCU. Options are:

- **MCU** - The device can act as a control unit for multipoint conferences
- **Gateway** - (MGC MCUs only) The device can act as a gateway for call management. MGC MCUs are not supported for this release. The MCU provides the capability if it registered successfully or is managed.

### Available to Schedule

Select this option to make the MCU available to users who are scheduling conferences.

### MCU (Network) Services

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H.323 Service</strong></td>
<td>Indicates a connection to an IP network using the H.323 protocol.</td>
</tr>
<tr>
<td><strong>IP (SIP)</strong></td>
<td>Indicates a connection to an IP network using the SIP protocol.</td>
</tr>
<tr>
<td><strong>H.323 &amp; SIP Service</strong></td>
<td>Indicates a connection to an IP network using both H.323 and/or SIP protocols</td>
</tr>
<tr>
<td><strong>H.320 Service</strong></td>
<td>Indicates a connection to an ISDN phone line using the H.320 protocol.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Name</th>
<th>A descriptive name for the network service.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Priority</th>
<th>The priority set for the network service as compared to other services when it was created.</th>
</tr>
</thead>
</table>

### MCU Resources

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Total Conferences</td>
<td>Maximum number of total conferences allowed at once on this MCU.</td>
</tr>
<tr>
<td>Max CP Conferences</td>
<td>Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.</td>
</tr>
<tr>
<td>Max Video Ports (RMX MCUs only)</td>
<td></td>
</tr>
<tr>
<td>Max Total Participants</td>
<td>Maximum number of total MCU participants allowed at once on this MCU.</td>
</tr>
<tr>
<td>Use Entry Queue</td>
<td>Indicates whether the MCU device supports an IVR.</td>
</tr>
<tr>
<td>Entry Queue Number ID</td>
<td>The IP number that conference participants dial to access the IVR prompt to join a conference.</td>
</tr>
<tr>
<td>Max CP Resolution</td>
<td>Set this to the highest available video format. Choices are: HD1080, CIF, SD15, SD30, and HD720. Refer to the RMX 2000/4000 Administrator’s Guide for more information about this field.</td>
</tr>
</tbody>
</table>

---

This document is a guide for Polycom RealPresence Resource Manager System Operations. It provides detailed information on capabilities, schedule availability, MCU network services, and MCU resources. The document is designed to help users configure and manage their Polycom systems effectively.
Add an MCU Manually

This topic describes how to add an MCU to a RealPresence Resource Manager system.

Back-end communication with the Polycom RMX system control units and IP service blades must be enabled.

When you add an MCU device, MCU network services are added automatically at the time the IP card registers with the RealPresence Resource Manager system.

When you add a gateway device, use the Services page to specify the network services available for the device.

- Polycom RMX system devices may only have H.323 service.
- Once an MCU registers with the RealPresence Resource Manager system, if you change an MCU service on the MCU, the update does not automatically get sent to the RealPresence Resource Manager system. To update the system, you must delete and read the MCU to the system.

When you enter network service information manually, remember that the RealPresence Resource Manager system does not create the service at the device. The service must have already been defined at the device. Enter information in the RealPresence Resource Manager system that matches the information in the device.

If you do not define network services, you may not use an MCU or gateway in a conference. For example, if you do not define the H.323 service on the MCU, when the RealPresence Resource Manager system tries to schedule a video conference that requires this service, it will look for another MCU with this service. If another MCU with this service is not available, the conference will not be scheduled.

To add an MCU bridge or find an MCU on the network

1. Go to Network Device > MCUs and click Add.
2 In the Add New Device dialog box, select the Device Type of interest.

3 Enter either the IP Address or the DNS Name of the MCU.

4 Enter the Admin ID and Password for the MCU.

5 Click Find Device.
   - If the RealPresence Resource Manager system can find the MCU on the network, the Add New Device dialog box is populated with information retrieved from the MCU. Review any information retrieved from the MCU.
   - If the RealPresence Resource Manager system cannot find the MCU on the network, a Device Not Found dialog box appears.

6 Click OK.

7 Complete the Identification, Addresses, Capabilities, MCU Services, MCU Resources, and MCU Cascading sections of the Add New Device dialog box.
   For more information, see “View Device Details” on page 229.
   At a minimum, assign the MCU a System Name.

When Integrating with a DMA System

- If your system integrates with a Polycom DMA system, make sure your MCU system name includes a qualifier that indicates to the DMA system administrator that the MCU is directly registered to the RealPresence Resource Manager system; for example, ResourceManager_RMX10.
- An RMX system can be managed by the RealPresence Resource Manager or the Polycom DMA system, not both.

Pay particular attention to the Capabilities options, because the settings on it determine how the MCU is used throughout the RealPresence Resource Manager system.

8 Click Add.

The MCU appears in the Network Device list. By default, the system:
   - Adds the MCU to the applicable site
   - Sets the HTTP Port to 80
   - Adds an Alias for the MCU
   - Makes the MCU Available to Schedule
   - Sets the Monitoring Level to Standard
Edit an MCU Bridge

To edit an MCU from the RealPresence Resource Manager system

1. Go to Network Device > MCUs.
2. As needed, use the Filter to customize the MCU list.
3. Select the MCU of interest and click Edit.
4. Complete the Identification, Addresses, Capabilities, MCU Services, MCU Resources, and MCU Cascading sections of the Edit Device dialog box.

At a minimum, assign the MCU a **System Name**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>The name of the MCU. The name must be unique. MCU names must be unique.</td>
</tr>
<tr>
<td></td>
<td>• The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid.</td>
</tr>
<tr>
<td></td>
<td>• When retrieved from the MCU, the name is taken from the H.323 ID if the MCU registered with the gatekeeper and it is a third-party system. In other cases, it is the system name, which might be different than the H.323 ID.</td>
</tr>
<tr>
<td>DNS Name</td>
<td>The DNS name of the MCU.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of MCU.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The assigned IP address of the MCU</td>
</tr>
<tr>
<td>Site</td>
<td>The network site for the MCU. By default, MCUs are added to the Primary Site.</td>
</tr>
<tr>
<td>Description</td>
<td>A free-form text field (Extended ASCII only) in which information about the MCU can be added</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number (ASCII only) of the MCU. The MCU provides the serial number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version of the software installed on the MCU (ASCII only). The MCU provides the version number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTP URL</td>
<td>(Polycom RMX systems only)</td>
</tr>
<tr>
<td></td>
<td>The management URL for the endpoint, if available (ASCII only). This URL allows the Resource Manager system to start the endpoint’s management system using the Manage function.</td>
</tr>
<tr>
<td></td>
<td>All Polycom endpoints allow device management through a browser. For these endpoints, this field is completed when the endpoint registers with the Resource Manager system.</td>
</tr>
<tr>
<td></td>
<td>For third-party endpoints that do not register using an IP address, you must enter the URL.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>(Polycom RMX systems only)</td>
</tr>
<tr>
<td></td>
<td>The HTTP port number for the MCU communications. The MCU provides the port number if it registered successfully and is managed.</td>
</tr>
<tr>
<td></td>
<td>By default, in non-secure (HTTP) mode, the RealPresence Collaboration Server uses port 80 and in secure (HTTPS) mode, the RealPresence Collaboration Server uses port 443.</td>
</tr>
<tr>
<td>Area</td>
<td>This field indicates the area in which the MCU resides.</td>
</tr>
<tr>
<td></td>
<td>This field is only visible when Areas are enabled and the user manages more than one area.</td>
</tr>
<tr>
<td></td>
<td>A user can only view area-specific information for an area(s) that he has permission to manage.</td>
</tr>
<tr>
<td>Addresses</td>
<td></td>
</tr>
<tr>
<td>ISDN Video Number</td>
<td>The country code + city/area code + phone number for the MCU.</td>
</tr>
<tr>
<td>Capabilities</td>
<td></td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>The communications protocols that the MCU can support. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP (H.323)</strong> - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ISDN (H.320)</strong> - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP (SIP)</strong> - A standard that defines the protocols used for multimedia communications on SIP networks. The MCU automatically provides the protocols if it registered successfully or is managed.</td>
</tr>
</tbody>
</table>

Polycom RealPresence Resource Manager System Operations Guide

236 Polycom, Inc.
### Capabilities Enabled

Capabilities to enable on this MCU. Options are:
- **MCU** - The device can act as a control unit for multipoint conferences
- **Gateway** - (MGC MCUs only) The device can act as a gateway for call management. MGC MCUs are not supported for this release.

The MCU provides the capability if it registered successfully or is managed.

### Available to Schedule

Select this option to make the MCU available to users who are scheduling conferences.

### MCU (Network) Services

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 Service</td>
<td>Indicates a connection to an IP network using the H.323 protocol.</td>
</tr>
<tr>
<td>IP (SIP)</td>
<td>Indicates a connection to an IP network using the SIP protocol.</td>
</tr>
<tr>
<td>H.323 &amp; SIP Service</td>
<td>Indicates a connection to an IP network using both H.323 and/or SIP protocols</td>
</tr>
<tr>
<td>H.320 Service</td>
<td>Indicates a connection to an ISDN phone line using the H.320 protocol.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>A descriptive name for the network service.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority set for the network service as compared to other services when it was created.</td>
</tr>
</tbody>
</table>

### MCU Resources

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Total Conferences</td>
<td>Maximum number of total conferences allowed at once on this MCU.</td>
</tr>
<tr>
<td>Max CP Conferences</td>
<td>Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.</td>
</tr>
<tr>
<td>Max Video Ports</td>
<td>(RMX MCUs only)</td>
</tr>
<tr>
<td>Max Total Participants</td>
<td>Maximum number of total MCU participants allowed at once on this MCU.</td>
</tr>
<tr>
<td>Use Entry Queue</td>
<td>Indicates whether the MCU device supports an IVR.</td>
</tr>
</tbody>
</table>
Delete an MCU Bridge

To delete an MCU from the RealPresence Resource Manager system

1. Go to Network Device > MCUs.
2. As needed, use the Filter to customize the MCU list.
3. Select the MCU of interest and click Delete.
4. Click Yes to confirm the deletion.

The MCU list is updated.

View Bridge Hardware

To view the hardware configuration of a bridge

1. Go to Network Device > MCUs.
2. As needed, use the Filter to customize the MCU list.
3. In the MCU list, select the bridge of interest and click View Hardware.

A Hardware pane appears below the bridge list. It lists the hardware for the selected bridge and displays the Slot number, Card Type, Status, Temperature, and Voltage for each piece of hardware.
View Bridge Services

To view the network services available on the bridge

1. Go to Network Device > MCUs.
2. As needed, use the Filter to customize the MCU list.
3. In the MCU list, select the bridge of interest and click View Services.
   
   A Services pane appears below the bridge list. It lists the network services for the selected bridge and identifies the Service Type, Service Name, and the default setting for the network service.

4. To view more details, select a service and click View.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>The name of the H.323 service (ASCII only) defined in the MCU.</td>
</tr>
<tr>
<td>Dialing Prefix</td>
<td>Prefix to select this service.</td>
</tr>
<tr>
<td>Service IP Address</td>
<td>IP address associated with this network service and with this H.323 card in the MCU.</td>
</tr>
<tr>
<td>Alias</td>
<td>Alias for the service defined in the MCU.</td>
</tr>
<tr>
<td>Note</td>
<td>Polycom recommends using E.164 as the alias for this service.</td>
</tr>
<tr>
<td></td>
<td>The number that is dialed if the endpoints are registered with the same gatekeeper. If the endpoints are not registered with the same gatekeeper, they use their assigned IP address to connect.</td>
</tr>
<tr>
<td>Port</td>
<td>Number of IP connections available.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority order for this service.</td>
</tr>
</tbody>
</table>

View Bridge Conferences

To view information about the conferences resident on the bridge

1. Go to Network Device > MCUs.
2. As needed, use the Filter to customize the MCU list.
3  In the MCU list, select the bridge of interest and click **View Conferences**. A **Conferences** pane appears below the bridge list. It lists the conferences for the selected bridge and identifies the conference **Status**, **Type**, **Conference Name**, **Start Time**, **Bridge**, **Creator** and **Area**.

The **Area** field is only visible when Areas are enabled and the user manages more than one area.

A user can only view area-specific information for an area(s) that he has permission to manage.

**View Bridge Ports**

To view information about the bridge ports

1  Go to **Network Device > MCUs**.

2  As needed, use the **Filter** to customize the MCU list.

3  In the MCU list, select the bridge of interest and click **View Ports**. A **Ports** pane appears below the bridge list. It lists the ports for the selected bridge and identifies the **Audio Ports Available**, **Video Ports Available**, **Audio Ports in Use**, and **Video Ports in Use**.

**View Bridge Meeting Rooms**

To view information about meeting rooms on a bridge

1  Go to **Network Device > MCUs**.

2  As needed, use the **Filter** to customize the MCU list.

3  In the MCU list, select the bridge of interest and click **View Meeting Rooms**. A **Meeting Rooms** pane appears below the bridge list. It lists the meeting rooms for the selected bridge and identifies the meeting room by **Name**, **ID**, **Duration**, **Conference**, **Chairperson**, **Chairperson Password**, and **Profile**.
View Bridge Entry Queues

To view information about entry queues on a bridge
1. Go to Network Device > MCUs.
2. As needed, use the Filter to customize the MCU list.
3. In the MCU list, select the bridge of interest and click View Entry Queues.

An Entry Queues pane appears below the bridge list. It lists the entry queues for the selected bridge and identifies the entry queue by Display Name, Routing Name, ID, Profile, and Dial-In Number.

View Bridge Gateway Conferences

To view information about gateway conferences on a bridge
1. Go to Network Device > MCUs.
2. As needed, use the Filter to customize the MCU list.
3. In the MCU list, select the bridge of interest and click View Gateway Conferences.

If the feature is available on the bridge, a Gateway Conferences pane appears below the bridge list. It lists the gateway conferences for the selected bridge.
MCU Device Details

This chapter identifies the fields found in the MCU Device Detail section of the Polycom® Polycom® RealPresence® Resource Manager system interface. It includes:

- “MCU H.320 Services” on page 243
- “MCU H.323 & SIP Services” on page 244
- “MCU Resources—Polycom RMX Platform” on page 245
- “MCU Device Summary Information” on page 246

Users with the Device Administrator role or Area Administrator role can view MCU device details.

### MCU H.320 Services

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU H.320 Service</td>
<td></td>
</tr>
<tr>
<td>Service Name</td>
<td>Name of the H.320 ISDN service</td>
</tr>
<tr>
<td>Channels</td>
<td>Number of 64K channels dedicated to the MCU</td>
</tr>
<tr>
<td>Number Range</td>
<td>Dial-in number range of service. These ISDN numbers are available on an MCU for all endpoints to use. Also called direct inward dialing (DID).</td>
</tr>
<tr>
<td>LCR Table</td>
<td>The least-cost routing table for calls made through this gateway</td>
</tr>
<tr>
<td>Local Prefix</td>
<td>The prefix required to place a call to a local number outside the enterprise. For example, if you dial 9 to reach an outside line, the <strong>Local Prefix</strong> is 9.</td>
</tr>
<tr>
<td>Non-Local Prefix</td>
<td>The prefix required to dial long distance. For example, in certain states in the United States, you must dial 1 before you can dial a non-local number.</td>
</tr>
</tbody>
</table>
### MCU H.323 & SIP Services

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>The name of the H.323 service (ASCII only) defined in the MCU.</td>
</tr>
<tr>
<td>Dialing Prefix</td>
<td>Prefix to select this service.</td>
</tr>
<tr>
<td>Service IP Address</td>
<td>IP address associated with this network service and with this H.323 card in the MCU.</td>
</tr>
<tr>
<td>Alias</td>
<td>Alias for the service defined in the MCU.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Polycom recommends using E.164 as the alias for this service.</td>
</tr>
<tr>
<td></td>
<td>The number that is dialed if the endpoints are registered with the same gatekeeper. If the endpoints are not registered with the same gatekeeper, they use their assigned IP address to connect.</td>
</tr>
<tr>
<td>Port</td>
<td>Number of IP connections available.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority order for this service.</td>
</tr>
</tbody>
</table>
** MCU Resources—Polycom RMX Platform **

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Total Conferences</td>
<td>Maximum number of total conferences allowed at once on this MCU.</td>
</tr>
<tr>
<td>Max CP Conferences</td>
<td>Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.</td>
</tr>
<tr>
<td>Max Video Ports</td>
<td>Maximum number of video ports on which participants can be connected.</td>
</tr>
<tr>
<td>Max Total Participants</td>
<td>Maximum number of total video participants allowed at once on this MCU.</td>
</tr>
<tr>
<td>Use Entry Queue</td>
<td>Indicates whether the RMX device supports an IVR.</td>
</tr>
<tr>
<td>Entry Queue Number ID</td>
<td>The number that conference participants dial to access the IVR prompt to join a conference.</td>
</tr>
<tr>
<td>Entry Queue ISDN Number</td>
<td>The number that conference participants dial to access the IVR prompt to join a conference.</td>
</tr>
</tbody>
</table>

**Audio & Video Settings:** The following parameters must be set manually to synchronize with the RMX device. See the RMX documentation for more information about these settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Voice Ports</td>
<td>Set this to the maximum number of audio ports configured on the RMX device.</td>
</tr>
<tr>
<td></td>
<td>Refer to the <em>RMX 2000/4000 Administrator’s Guide</em> for more information about this field.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Up to 10 blocks of RMX video ports can be converted to 50 audio-only ports, up to a maximum of 200 audio-only ports.</td>
</tr>
<tr>
<td>Max CP Resolution</td>
<td>Set this to the highest available video format. Choices are: HD1080, CIF, SD15, SD30, and HD720.</td>
</tr>
<tr>
<td></td>
<td>Refer to the <em>RMX 2000/4000 Administrator’s Guide</em> for more information about this field.</td>
</tr>
<tr>
<td>Max Bandwidth Capacity (Kbps)</td>
<td>The maximum bandwidth to the Polycom RMX system.</td>
</tr>
</tbody>
</table>
# MCU Device Summary Information

The **Device Summary** information for MCUs in the **Monitor View** section includes the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of device.</td>
</tr>
<tr>
<td>ID</td>
<td>The system-generated ID for the device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The assigned IP address of the device.</td>
</tr>
<tr>
<td>Area</td>
<td>Area with which the device is associated. This field is only available when Areas are enabled and the RealPresence Resource Manager user is given a role that allows them to view area information.</td>
</tr>
<tr>
<td>ISDN Video Number</td>
<td>For ISDN devices only, the country code + city/area code + phone number for the device. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The Resource Manager system only supports native ISDN.</td>
</tr>
<tr>
<td>Site</td>
<td>The network site for the device. By default, devices are added to the <strong>Primary Site</strong>.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number (ASCII only) of the device. The device provides the serial number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Available to Schedule</td>
<td>Select this option to make the device available when users are scheduling conferences.</td>
</tr>
</tbody>
</table>

**Note**

When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.

**Available to schedule** field is disabled for RMX devices.
### Supported Protocols

The communications protocols that the device can support. Possible values include:

- **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP.
- **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.
- **SIP** - A standard that defines the protocols used for multimedia communications on SIP networks.

The device automatically provides the protocols if it registered successfully or is managed.

### Capabilities Enabled

Capabilities to enable on this device. Options are:

- **MCU** - The device can act as a control unit for multipoint conferences
- **Gateway** - The device can act as a gateway for call management

The MCU provides the capability if it registered successfully or is managed.

**Note**

Currently, RMX MCUs cannot be Gateway devices.

### Alias (type)

The alias to connect to the device. The Resource Manager system converts the aliases to the IP address associated with the device.

- **Alias Type**. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown.
- **Alias Value**. Value for the alias type shown.
- The value for the H.323 ID is the device name if the device registered with the gatekeeper and it is a third-party system. In other cases, the device name is the system name, which might be different than the H323 ID.
- The value of the E.164 alias is the extension dialed to reach this endpoint.
- To add another alias, select the type, enter the value (ASCII only), and click Add Alias.
- To remove an alias, select it and click Delete Selected Row.

**Note**

The following Alias Values are ASCII only: H323 ID, URL, Transport Address, and Unknown.
Managing a DMA System

This chapter describes how to perform the Polycom® RealPresence® Resource Manager system network device management tasks. It includes:

- Using a Polycom DMA System with RealPresence Resource Manager System
- Integrating with a Polycom DMA System
- Managing DMA Pool Orders

For this release, Polycom supports integrating your RealPresence Resource Manager system with a Polycom DMA system v5.0 or later.

Using a Polycom DMA System with RealPresence Resource Manager System

You can integrate your RealPresence Resource Manager system with a Polycom DMA system to take advantage of the DMA system’s two main functions: Conference Manager function and the Call Server (gatekeeper and SIP proxy/registrar) function, described below.

- Conference Manager
  - Provides a highly reliable and scalable multipoint conferencing solution that distributes voice and video calls across multiple media servers (MCUs), creating a single seamless resource pool. The system essentially behaves like a single large MCU, which greatly simplifies video conferencing resource management and improves efficiency.
  - Supports up to 64 MCUs. MCUs can be added on the fly without impacting end users and without requiring re-provisioning.

- Call Server
— Provides complete endpoint registration and call routing services for both H.323 and SIP protocols. It also serves as a gateway between H.323 and SIP, enabling enterprises with legacy H.323 devices to transition to SIP in a gradual, orderly, and cost-effective manner.

— Provides bandwidth management, and can be integrated with a Juniper Networks Session and Resource Control Module (SRC) to provide bandwidth assurance services.

— Comes with a default dial plan that covers many common scenarios, but which can easily be modified.

The Call Server makes it possible for multiple UC environments and different video conferencing technologies to be unified across the network into a single dial plan.

See the Polycom DMA 7000 System Operations Guide for more information.

This section includes the following topics that discuss some of the considerations when integrating a DMA system with your RealPresence Resource Manager system.

• “SIP Endpoint Management” on page 250
• “Conference Types Supported By the DMA System” on page 251
• “Considerations for Site Topology” on page 251
• “Scheduling Capacity” on page 252

SIP Endpoint Management

For SIP-only endpoints that register with the DMA system and do not register with the RealPresence Resource Manager system’s provisioning service, you must manually add them to the RealPresence Resource Manager system in order to manage that endpoint.

H.323 endpoints that register with the DMA system’s gatekeeper automatically display in a RealPresence Resource Manager system that has been configured with a DMA system.

MCU Management

• When your system integrates with a Polycom DMA system, make sure the names of MCU systems that are managed by the RealPresence Resource Manager includes a qualifier that indicates to the DMA system administrator that the MCU is directly registered to the RealPresence Resource Manager system; for example, ResourceManager_RMX10.

• An RMX system can be managed by the RealPresence Resource Manager or the Polycom DMA system, not both.
Conference Types Supported By the DMA System

You need to integrate with a Polycom DMA system in order to support the following RealPresence Resource Manager system conference types:

- **Anytime Conferences** are conferences that are initiated when the conference owner dials in and where most other participants are dial-out participants. Conference templates for anytime conferences are created and maintained on the DMA system.

- **Pooled Conferences** are conferences that are scheduled on resources managed by the Polycom DMA system. Conference templates for pooled conferences are created and maintained on the DMA system.

DMA Conference Templates

You need to have created DMA conference templates for schedulers to use when scheduling either a pooled conference (future) or anytime conference. You do this in the DMA system.

As a best practice, use a naming convention that helps identify the appropriate use for the conference template. For example, you can name conference templates intended for anytime conferences with an “anytime” prefix such as `anytime_corptemplate`.

Multi-Tenancy Considerations

DMA system conference templates are not area-aware, which means they cannot be associated with a particular area. An area scheduler can select any DMA system conference template to use for a conference.

As a best practice, you should use a naming convention that helps the scheduler identify the correct template to use for his area conferences.

Considerations for Site Topology

When integrated with the RealPresence Resource Manager system, the Polycom DMA system inherits site topology settings from the RealPresence Resource Manager system. Site topology configuration for both products is managed by a RealPresence Resource Manager system user with the administrator role.

When the RealPresence Resource Manager system is integrated with a DMA system, you should plan your site topology with DMA system needs in mind. For example, when your DMA system uses a supercluster environment, territories have specific functional roles. It’s important to work with your DMA system administrator to ensure the site topology meets your environments needs.

See the *Polycom DMA 7000 System Operations Guide* for more information.
**Scheduling Capacity**

You can tune the scheduling capacity of the DMA system that the RealPresence Resource Manager system relies on. You do this through the RealPresence Resource Manager system.

The number of ports used for a conference can vary according to the MCU that hosts the conference and the number/type of endpoints that join. Because schedulers can only choose from a pre-configured DMA system pool order when scheduling pooled conferences, they rely on an administrator to tune the DMA system’s scheduling capacity to ensure efficient use of resources.

There are three ways an administrator can assess DMA system scheduling capacity:

- View conference reports from the DMA system. This method is preferred and provides the most accurate information.
- Monitor ongoing conferences to assess if resources were underbooked.
- View information on RealPresence Resource Manager CDR reports to review ports used for individual conferences.

Polycom recommends setting the DMA system scheduling capacity more conservatively at first and then tuning for increased conference activity. See “Edit a Polycom DMA System” on page 254.

**Integrating with a Polycom DMA System**

You can integrate your RealPresence Resource Manager with a Polycom DMA system. This section includes these topics:

- “DMA View” on page 252
- “Add a Polycom DMA System” on page 253
- “Edit a Polycom DMA System” on page 254
- “Delete a Polycom DMA System” on page 254

**DMA View**

Use the DMA View to view Polycom DMA systems v5.0 or later. You can integrate your RealPresence Resource Manager with these later versions of the DMA system for both call server (gatekeeper and SIP proxy/registrar) and MCU pool order capability.

The DMA system list has the following information.
Add a Polycom DMA System

RealPresence Resource Manager system users with the Device Administrator role can add a Polycom DMA system to a RealPresence Resource Manager system.

To add a Polycom DMA system

1. Go to Network Device > DMA and click Add.
2. In the Add DMA dialog box, enter a unique and identifying Name and Description for the DMA system.
3. Enter the IP Address/Hostname. This field can be either the IP address of the DMA system or the DNS host name (FQDN).
   For DMA systems with multiple clusters, indicate the FQDN of the cluster you want to use.
   If your DMA system is configured for a super cluster, be sure to use the Virtual IP address for a cluster that is co-located with the RealPresence Resource Manager.
4. Enter the Port used to access the DMA system. The default port is 8443.
5. Enter the Username and Password for the DMA system.
   The DMA system user you use to authenticate the DMA system must have the Administrator role and gold class of service.
6. Mark the applicable check boxes in the Used As field.
   You can use your DMA system as both of the following:
   - a Call Server (gatekeeper)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMA Name</td>
<td>A unique name for the DMA system.</td>
</tr>
<tr>
<td>Description</td>
<td>A useful description for the Polycom DMA system.</td>
</tr>
<tr>
<td>IP Address/Hostname</td>
<td>The virtual IP address for the DMA system. For DMA systems with multiple clusters, indicate the FQDN of the cluster you want to use. If your DMA system is configured for a super cluster, be sure to use the Virtual IP address for a cluster that is co-located with the RealPresence Resource Manager.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used to access the DMA system. The default port is 8443.</td>
</tr>
<tr>
<td>MCU Pool Orders</td>
<td>A check mark displays if the DMA system has been enabled for MCU pool orders (conference management).</td>
</tr>
<tr>
<td>Call Server</td>
<td>A check mark displays if the DMA system has been enabled for use as a call server (gatekeeper).</td>
</tr>
</tbody>
</table>
Define the **Scheduling Capacity** as a percentage of total capacity.

For more information about scheduling capacity, see “Scheduling Capacity” on page 252.

Click **Add**.

The DMA system appears in the **Network Device** list.

### Edit a Polycom DMA System

You must have the Device Administrator role in order to edit a Polycom DMA system.

**To edit a DMA system**

1. Go to **Network Device > DMA**.
2. Select the DMA system and click **Edit**.
3. In the **Edit DMA** dialog box, edit the properties of the DMA system.
4. Click **OK**.

### Delete a Polycom DMA System

You must have the Device Administrator role in order to delete a Polycom DMA system.

**To delete a DMA system from a RealPresence Resource Manager system**

1. Go to **Network Device > DMA**.
2. Select the DMA system and click **Delete**.
3. Click **Yes** to confirm the deletion.

### Managing DMA Pool Orders

When the RealPresence Resource Manager system is configured to work with a Polycom DMA system, conference schedulers can schedule conferences on DMA system pool orders.

DMA system pool orders associated with your configured DMA system are automatically displayed in the RealPresence Resource Manager system.
The DMA system administrator is responsible for setting up pool orders to be used. You should work with your DMA system administrator to determine the specifics about the pool orders associated with your DMA system. This information can also be useful for schedulers who need to choose a pool order to use for a conference.

DMA Pool Orders are groups of MCU pools that are hierarchically organized. Some uses for DMA system pool orders:

• The DMA system administrator can put all MCUs in a specific site or domain into a pool. Then, assign a pool order to all users in that site or domain (via group membership) ensuring that their conferences are preferentially routed to MCUs in that pool.

• The DMA system administrator could put one or more MCUs into a pool to be used only by executives, and put that pool into a pool order associated only with those executives’ conference rooms.

• The DMA system administrator could put MCUs with special capabilities into a pool, and put that pool into a pool order associated only with custom conference rooms requiring those capabilities.

For more information about pool orders, see the *Polycom DMA 7000 System Operations Guide*.

This section includes the following topics:

• View Details of a DMA System Pool Order

• Associate a Polycom DMA System Pool Order with an Area

**View Details of a DMA System Pool Order**

You can use the RealPresence Resource Manager system to view DMA system Pool Order details. You cannot modify these properties. DMA system pool orders are created on the DMA system by a DMA system administrator.

**To view details a DMA System Pool Order**

1. Go to **Network Device > DMA Pool Orders**.
2. Select the DMA system pool order of interest.

   The **DMA Pool Order Detail** pane is populated with the details for the selected pool order. These details are configured on the DMA system and cannot be modified with the RealPresence Resource Manager system.
Users with Device Administrator role can associate a DMA pool order with an area.

When you do this, only schedulers belonging to that area can schedule conferences for that DMA system pool order. The advanced scheduler or area operator must either be in the same area as the DMA system pool order or be able to manage the area in which the DMA system pool order resides.

Schedulers and area schedulers cannot select particular resources on which to schedule conferences.

### To associate a DMA System Pool Order with an Area

1. Go to **Network Device > DMA Pool Orders**.
2. Select the **DMA Pool Order** of interest and click **Associate Areas**.
3. In the **Available Areas** section, select and move the desired area(s) to **Selected Areas** list. You can move the unwanted area(s) to the **Available Areas** list. Press **Shift-click** or **Ctrl-click** to select multiple items in the list.
   - You must have the Device Administrator role to associate a DMA system pool order with an area. The **Available Areas** list is limited to the areas that you manage.
4. Click **OK**.
Managing Border Controllers and Firewalls

This chapter describes how to perform the Polycom® RealPresence® Resource Manager system network device management tasks. It includes:

- “Manage Polycom VBP Devices” on page 257
- “Manage SBC Devices” on page 260

Manage Polycom VBP Devices

The Polycom Video Border Proxy (VBP) device management operations include these topics:

- “VBP View” on page 258
- “Add a Polycom VBP Device” on page 258
- “Copy the RealPresence Resource Manager System Certificate to a Polycom VBP Device” on page 259
- “Edit a Polycom VBP Device” on page 259
- “Delete a Polycom VBP Device” on page 259
- “Identify Endpoints Using the Polycom VBP Device” on page 260
VBP View

Use the **VBP View** to manage Polycom Video Border Proxy™ (VBP™) firewall devices on the network.

Polycom VBP devices, when installed at the edge of the operations center, secures critical voice, video, and data infrastructure components including VoIP softswitches, video gatekeepers, gateways, media servers, and endpoints.

The Polycom VBP 5300 or 6400 S/T platform has an access proxy feature that provides firewall traversal that enables the RealPresence Resource Manager system dynamic management features across a firewall.

The **VBP** list has the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the Polycom VBP device.</td>
</tr>
<tr>
<td>Model</td>
<td>The model of Polycom VBP device.</td>
</tr>
<tr>
<td>Provider-side IP</td>
<td>The private network IP address for the Polycom VBP device.</td>
</tr>
<tr>
<td>Subscriber-side IP</td>
<td>The public network IP address for the Polycom VBP device.</td>
</tr>
</tbody>
</table>

**Add a Polycom VBP Device**

**IMPORTANT**

When you add a new Polycom VBP device, the RealPresence Resource Manager system will restart the user interface web service. This will interrupt others using the Resource Manager system user interface.

**To add a Polycom VBP device to a RealPresence Resource Manager system**

1. Go to **Network Device > VBPs** and click **Add**.
2. Configure these settings in the **Add VBP** dialog box.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the Polycom VBP device.</td>
</tr>
<tr>
<td>Provider-side IP</td>
<td>The Private Network IP address for the Polycom VBP device.</td>
</tr>
<tr>
<td>Subscriber-side IP</td>
<td>The Public Network IP address for the Polycom VBP device.</td>
</tr>
</tbody>
</table>
3 Click OK.

A system dialog box appears indicating that you must restart Apache for the settings to take affect. You also have the opportunity to add another Polycom VBP device.

The Polycom VBP device is added to the RealPresence Resource Manager system. However, more configuration may be necessary for the device to operate in your network. For example, you will probably need to “Copy the RealPresence Resource Manager System Certificate to a Polycom VBP Device” as described in the next topic.

**Copy the RealPresence Resource Manager System Certificate to a Polycom VBP Device**

**To copy the RealPresence Resource Manager system certificate to a Polycom VBP device**

1 Go to Network Device > VBPs
2 Select the Polycom VBP device of interest and click **Copy Certificate to VBP**.
   In the **Copy Certificate to VBP** dialog box, the system automatically populates the **Filename** field with the filename of the RealPresence Resource Manager system certificate and the **Username** field with root.
3 Enter the SSH or console **Password** for the root user and click **OK**.
   The Polycom VBP device appears in the **Network Device** list.

**Edit a Polycom VBP Device**

**To edit a Polycom VBP device**

1 Go to Network Device > VBPs
2 Select the Polycom VBP device of interest and click **Edit**.
3 Configure these settings as needed in the **Edit VBP** dialog box.
4 Click **OK**.

**Delete a Polycom VBP Device**

**To delete a Polycom VBP device from a RealPresence Resource Manager system**

1 Go to Network Device > VBPs.
Select the Polycom VBP device of interest and click **Delete**.

Click **Yes** to confirm the deletion.

### Identify Endpoints Using the Polycom VBP Device

This procedure identifies only Polycom HDX and CMA Desktop systems that are:

- Registered to the RealPresence Resource Manager system
- Using the Polycom VBP firewall
- Operating in dynamic-management mode.

One Polycom HDX or legacy endpoint system operating in standard management mode, registered to the RealPresence Resource Manager system, and using the Polycom VBP firewall may also be displayed in the **Endpoint** list. This entry may represent multiple endpoints, since all Polycom HDX or legacy endpoint system operating in standard management mode register with the same information.

To identify which endpoints are using the Polycom VBP firewall

1. Go to **Endpoint > Monitor View**.
2. Click **Select Filter** and select **IP Address**.
3. Enter the provider-side IP address of the Polycom VBP device and press **Enter**.

   The **Endpoint** list displays the dynamically-managed endpoints that are registered to the RealPresence Resource Manager system and using the Polycom VBP firewall. All of the endpoints display the same IP address, which is the Provider-side IP address of the Polycom VBP device. However, the endpoints will have different aliases and owners.

### Manage SBC Devices

Polycom supports the use of the Acme Packet Net-Net Enterprise Session Director session border control with the RealPresence Resource Manager system.

The SBC device management operations include these topics:

- **Add a SBC Device**
- **Edit a SBC Device**
- **Delete an SBC Device**
- **Identify Endpoints Using the SBC Device**
Add a SBC Device

Polycom supports the use of the Acme Packet Net-Net Enterprise Session Director session border control with the RealPresence Resource Manager system.

To add a SBC device to a RealPresence Resource Manager system
1. Go to Network Device > SBCs and click Add.
2. Configure these settings in the Add SBC dialog box.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the SBC.</td>
</tr>
<tr>
<td>Provider-side IP</td>
<td>The Private Network IP address for the SBC device.</td>
</tr>
<tr>
<td>Subscriber-side IP</td>
<td>The Public Network IP address for the SBC device.</td>
</tr>
</tbody>
</table>

3. Click OK.

The SBC device is added to the RealPresence Resource Manager system. However, more configuration may be necessary for the device to operate in your network.

You also have the opportunity to add another SBC device.

Edit a SBC Device

To edit a SBC device
1. Go to Network Device > SBCs.
2. Select the SBC device of interest and click Edit.
3. Configure these settings as needed in the Edit SBC dialog box.
4. Click OK.

Delete an SBC Device

To delete a SBC device from a RealPresence Resource Manager system
1. Go to Network Device > SBCs.
2. Select the SBC device of interest and click Delete.
3. Click Yes to confirm the deletion.
Identify Endpoints Using the SBC Device

**Note**
This procedure identifies only Polycom HDX systems and RealPresence Mobile that are:
- Registered to the RealPresence Resource Manager system
- Using the SBC device
- Operating in dynamic-management mode.

To identify which endpoints are using the SBC firewall
1. Go to Endpoint > Monitor View.
2. Click Select Filter and select IP Address.
3. Enter the provider-side IP address of the SBC device and press Enter.

The Endpoint list displays the dynamically-managed endpoints that are registered to the RealPresence Resource Manager system and using the SBC firewall. All of the endpoints display the same IP address, which is the Provider-side IP address of the SBC device. However, the endpoints will have different aliases and owners.
The Polycom® RealPresence® Resource Manager system supports two types of users.

- Users that come directly from the enterprise directory from which users are imported. These users are referred to as **enterprise users**.
- Users that are local to the management system. These users are added manually to the system.

Both user types can be assigned management roles, associated with endpoints, and organized in groups.

By default all users can be scheduled into conferences, and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

This chapter provides an overview of the Polycom® RealPresence® Resource Manager system users and groups management structure. It includes these topics:

- “Working with Users” on page 263
- “Working with Groups” on page 265
- “Working with Management Roles and Permissions” on page 266

### Working with Users

The RealPresence Resource Manager system supports two types of users.

- Users that come directly from the enterprise directory from which users are imported. These users are referred to as **enterprise users**.
- Users that are local to the management system. These users are added manually to the system.
Local Users

When you manually add local users, the RealPresence Resource Manager system manages all user information and associations.

At a minimum, when you manually add users, you must enter a user’s First Name or Last Name, User ID, Email Address, and Password. When you enter the minimum information, the RealPresence Resource Manager system automatically assigns local users the basic Scheduler role or Area Scheduler role (when areas are enabled), unless you remove that assignment. You can unassign that role if the user does not need any management permissions.

By default all users can be scheduled into conferences, and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

You can associate local users with one or more roles and associate them with one or more endpoints. Alternatively, you can associate local users with roles by associating them with local groups, see “Local Groups” on page 265.

If your company has implemented multi-tenancy, you can also associate local users with areas for which you manage. For more information about areas, see “Configuring Multi-Tenancy” on page 397 or “Managing Areas” on page 409.

Enterprise Users

When the RealPresence Resource Manager system is integrated with an enterprise directory, the system manages only the following pieces of an enterprise users’ information:

- Endpoints associated with the user
- Roles assigned to the user
- Area to which the user belongs
- Alert profiles for the user

The remaining information is pulled from the enterprise directory, including E-mail address, system password and so on.

Currently, the RealPresence Resource Manager system supports only a Microsoft Active Directory implementation of an LDAP directory.

The RealPresence Resource Manager system displays a user’s City, Title, and Department to help distinguish between users with the same name.

Users imported into the system through the enterprise directory are by default added to the system without a role. This default set up allows users to log into the RealPresence Resource Manager system with their enterprise user IDs and passwords. They can then be scheduled into conferences and call into conferences. However, the system cannot call out to them until they are associated with endpoints.
Assign Roles to Enterprise Users

You must decide which users will have management roles. Users with management roles can perform tasks on the RealPresence Resource Manager system, such as device management or conference scheduling. Management roles can be system-wide or area-restricted. A user must be assigned a management role in order to access the management system interface.

Conference participant users can be scheduled into conferences do not need to be assigned a management role, unless that particular user also needs to perform system management tasks.

If your company has implemented the Areas feature, you can also associate enterprise users with areas for which you are an administrator. For more information about areas, see “Managing Areas” on page 409 or “Configuring Multi-Tenancy” on page 397.

If you want the RealPresence Resource Manager system to, by default, to automatically assign enterprise users the basic Scheduler role, you must change the appropriate system Security Settings. See “Give Enterprise Users Default Scheduler Role” on page 457.

Working with Groups

Groups provide a more efficient and consistent use of the RealPresence Resource Manager system, because they allow you to assign roles and provisioning profiles to sets of users rather than to individual users.

This section includes the following topics:

• “Local Groups” on page 265
• “Enterprise Groups” on page 265

Local Groups

The RealPresence Resource Manager system allows you to add local groups (that is, groups added manually to the system) and associate them with provisioning profiles and roles.

For local groups, the RealPresence Resource Manager system manages all group information and associations.

Enterprise Groups

When the RealPresence Resource Manager system is integrated with an enterprise directory, groups defined to the enterprise directory are not automatically added to the RealPresence Resource Manager system, but you can import them into the system.
When the RealPresence Resource Manager system is integrated with an enterprise directory, the system manages only three pieces of group information: the provisioning profile assigned to the group, the roles assigned to the group, and whether or not the group is Directory Viewable (that is, displayed in endpoint directories). The remaining group information is pulled from the enterprise directory.

**Prepare to Use Active Directory**

To take full advantage of the RealPresence Resource Manager system, the enterprise Microsoft Active Directory must:

- Have Global Catalog turned ON. The Global Catalog enables searching for Active Directory objects in any domain without the need for subordinate referrals, and users can find objects of interest quickly without having to know what domain holds the object.
- Use universal groups. The Global Catalog stores the member attributes of universal groups only. It does not store local or global group attributes.
- Have a login account that has read access to all domains in the Active Directory that the RealPresence Resource Manager system can use. We recommend an account with a administrative username and a non-expiring password.
- Have the Active Directory Domain Name Service correctly configured. For more information about Active Directory design and deployment, see the Microsoft best practices guides at http://technet.microsoft.com.

For system and endpoint directory performance purposes, two best practices in regards to enterprise groups are:

- Do not import more than 500 enterprise groups into a RealPresence Resource Manager system.
- Do not mark more than 200 enterprise groups as Directory Viewable.

**Working with Management Roles and Permissions**

You must decide which users will have management roles. Users with management roles can perform tasks on the RealPresence Resource Manager system, such as device management or conference scheduling. Management roles can be system-wide or area-restricted. A user must be assigned a management role in order to access the management system interface.

Participant users who can be scheduled into conferences do not need to be assigned a management role, unless that particular user also needs to perform system management tasks.

For more information about area roles, see “User Roles within a Multi-Tenancy Environment” on page 398.
Understanding User Roles

The RealPresence Resource Manager system is a role and permissions based system.

- Users can assigned one or more user roles either directly or through their group associations.
- User roles are assigned a set of permissions. The system comes with default roles for both system-wide and area management tasks.
- Users see only the pages and functions available to their roles and associated permissions. Permissions are cumulative, so users see all of the pages and functions assigned to all of their roles and associated permissions.

- Users inherit roles from their parent groups—local or enterprise. They cannot inherit roles from groups more distantly removed—for example, from their grandparent groups.
- The default role names are stored in the system database and are not localized into other languages. If you wish to localized their names into your language, edit the roles and enter new names for them.

- If your company has implemented the Areas feature, users are restricted to the manage resources in the areas they are assigned to manage, according to the role they are given.

While the RealPresence Resource Manager system allows businesses almost unlimited flexibility in defining roles, for simplicity and clarity, we recommend keeping the default roles with their default permissions and responsibilities. Because users can be assigned multiple roles, and permissions are cumulative, your business can combine roles as needed to reflect the workload your people undertake to manage and use the system.

An administrator has several options when implementing user roles.

1. Implement only the default user roles and keep the standard permissions assigned to these roles.

2. Implement only the default user roles but change the permissions assigned to these roles.
3 Implement either option 1 or 2, but also create additional unique, workflow-driven user roles and determine which permissions to assign to those user roles.

Some important notes about user roles and permissions:

- Users (local and enterprise) may be assigned more than one role. In this case, the permissions associated with those roles are cumulative; a user has all of the permissions assigned to all of his roles.

- Users (local and enterprise) may be assigned roles as an individual and as part of a group. Again, the permissions associated with those roles are cumulative; a user has all of the permissions assigned to all of his roles no matter how that role is assigned.

- Users assigned a role with any one of the Administrator Permissions are generally referred to as administrators. Users assigned a role with any one of the Operator Permissions and none of the Administrator Permissions are referred to as Operators. Users assigned a user role with Scheduler Permissions and none of the Administrator or Operator Permissions are referred to as Schedulers.

### Default System Roles and Permissions

The RealPresence Resource Manager system includes a default set of management roles. Roles are associated with a set of permissions that allow the user to perform certain management tasks. Users see only the menus, pages, and functions associated with their roles.

While the RealPresence Resource Manager system allows administrators almost unlimited flexibility in defining roles, for simplicity and clarity, we recommend keeping the default roles with their default permissions and responsibilities. Because users can be assigned multiple roles, and permissions are cumulative, your business can combine roles as needed to reflect the workload your people undertake to manage and use the system.

The following table identifies the default system roles. Each of these roles is discussed in more detail in the following sections:

- “Scheduler Roles, Responsibilities, and Menus” on page 271
- “Operator Role, Responsibilities, and Menus” on page 272
- “Device Administrator Role, Responsibilities, and Menus” on page 272
- “Auditor Role, Responsibilities, and Menus” on page 273
- “Administrator Role, Responsibilities, and Menus” on page 274
For information about area roles, see “User Roles within a Multi-Tenancy Environment” on page 398.

The default role names are stored in the system database and are not localized into other languages. If you wish to localized the role names into your language, edit the roles and enter new names for them.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler</td>
<td>Schedule Conferences</td>
</tr>
<tr>
<td></td>
<td>Scheduling Level = Basic</td>
</tr>
<tr>
<td></td>
<td><strong>When areas are enabled:</strong></td>
</tr>
<tr>
<td></td>
<td>View and/or modify all areas.</td>
</tr>
<tr>
<td></td>
<td>Can perform role tasks in all areas.</td>
</tr>
<tr>
<td>Advanced Scheduler</td>
<td>Schedule Conferences</td>
</tr>
<tr>
<td></td>
<td>Scheduling Level = Advanced</td>
</tr>
<tr>
<td></td>
<td><strong>When areas are enabled:</strong></td>
</tr>
<tr>
<td></td>
<td>View and/or modify all areas.</td>
</tr>
<tr>
<td></td>
<td>Can perform role tasks in all areas.</td>
</tr>
<tr>
<td>View-Only Scheduler</td>
<td>Schedule Conferences</td>
</tr>
<tr>
<td></td>
<td>Scheduling Level = View-Only</td>
</tr>
<tr>
<td></td>
<td><strong>When areas are enabled:</strong></td>
</tr>
<tr>
<td></td>
<td>View and/or modify all areas.</td>
</tr>
<tr>
<td></td>
<td>Can perform role tasks in all areas.</td>
</tr>
<tr>
<td>Operator</td>
<td>Conference Operator</td>
</tr>
<tr>
<td></td>
<td>Report Operator</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting</td>
</tr>
<tr>
<td></td>
<td>Schedule Conferences</td>
</tr>
<tr>
<td></td>
<td>Scheduling Level = Advanced</td>
</tr>
<tr>
<td></td>
<td><strong>When areas are enabled:</strong></td>
</tr>
<tr>
<td></td>
<td>View and/or modify all areas.</td>
</tr>
<tr>
<td></td>
<td>Can perform role tasks in all areas.</td>
</tr>
</tbody>
</table>
### Role Permissions

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Administrator</td>
<td>Add endpoints and network devices.</td>
</tr>
<tr>
<td></td>
<td>Network Device Admin</td>
</tr>
<tr>
<td></td>
<td><strong>When areas are enabled:</strong></td>
</tr>
<tr>
<td></td>
<td>View and/or modify all areas.</td>
</tr>
<tr>
<td></td>
<td>Place devices and endpoints in Areas</td>
</tr>
<tr>
<td>Administrator</td>
<td>Directory Setup</td>
</tr>
<tr>
<td></td>
<td>Topology Setup</td>
</tr>
<tr>
<td></td>
<td>Conferencing Setup</td>
</tr>
<tr>
<td></td>
<td>System Setup</td>
</tr>
<tr>
<td></td>
<td>Create Areas (when activated)</td>
</tr>
<tr>
<td></td>
<td>Network Device Monitor</td>
</tr>
<tr>
<td></td>
<td>System Maintenance/Troubleshooting</td>
</tr>
<tr>
<td></td>
<td>Provision Profiles</td>
</tr>
<tr>
<td></td>
<td>Create software updates</td>
</tr>
<tr>
<td></td>
<td>Network device monitor</td>
</tr>
<tr>
<td></td>
<td><strong>When areas are enabled:</strong></td>
</tr>
<tr>
<td></td>
<td>Assign Resource Manager users to manage areas</td>
</tr>
<tr>
<td></td>
<td>Place Entities in areas</td>
</tr>
<tr>
<td></td>
<td>View and/or modify all areas</td>
</tr>
<tr>
<td>Auditor</td>
<td>Auditor</td>
</tr>
</tbody>
</table>

*Note* This role cannot be deleted or edited.

Most users will also see these menu items:

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings.</strong> Click here to display a <strong>Settings</strong> dialog box with the following information:</td>
</tr>
<tr>
<td>• User Name</td>
</tr>
<tr>
<td>• Remote Server</td>
</tr>
<tr>
<td>• Software Version</td>
</tr>
<tr>
<td>• Font Size</td>
</tr>
<tr>
<td>In this dialog box, you can also:</td>
</tr>
<tr>
<td>• Change the font size used in your display of the RealPresence Resource Manager system web client interface.</td>
</tr>
<tr>
<td>• Change your password, if you are a local system user.</td>
</tr>
</tbody>
</table>

| Downloads.** Click here to display the **Downloads** dialog box with the downloadable applications that are compatible with the RealPresence Resource Manager system. Downloadable applications include: |
| • CMA Desktop client for PC or MAC (including the path to the application)  |
| • Polycom File Verification Utility |
Scheduler Roles, Responsibilities, and Menus

The RealPresence Resource Manager system offers three different default Scheduler roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler</td>
<td>For the areas to which they belong (areas are optional), users assigned the <strong>Scheduler</strong> (sometimes called basic scheduler) role can schedule conferences. They do so using the conference templates defined for them. But basic schedulers cannot change any of the conference settings defined in the templates they choose when scheduling their conferences.</td>
</tr>
<tr>
<td>Advanced Scheduler</td>
<td>For the areas to which they belong (areas are optional), users assigned the <strong>Advanced Scheduler</strong> role can also schedule conferences. And again they do so using the conference templates defined for them. But advanced schedulers can change selected conference settings defined in the template they use when scheduling their conferences.</td>
</tr>
<tr>
<td>View-Only Scheduler</td>
<td>For the areas to which they belong (areas are optional), users assigned the <strong>View-only Scheduler</strong> role cannot schedule conferences; they can only see conferences that have been scheduled.</td>
</tr>
</tbody>
</table>

When basic or advanced schedulers log into the RealPresence Resource Manager system, the system displays the **Future** conference page and they have access to the following menu items:

- **Log Out.** Click here to log out of the RealPresence Resource Manager system.
- **Note**
  - The RealPresence Resource Manager system has an inactivity timer. If you are logged into the system but do not use the interface for a specified period of time (10 minutes by default), the system automatically logs you out.
- **Help.** Links to the RealPresence Resource Manager system online help.
When view-only schedulers log into the RealPresence Resource Manager system, the system displays the **Ongoing** conference page and it is the only menu item to which they have access.

**Operator Role, Responsibilities, and Menus**

The **Operator** role allows businesses to offer high-touch customer service for video conferencing. User assigned the **Operator** role can:

- Schedule conferences.
- Monitor and manage ongoing conferences.
- Monitor endpoints.
- Monitor network devices such as MCUs.
- Add, edit, and delete entries in the system **Guest Book**.
- Create favorites.
- View some system reports.

When operators log into the RealPresence Resource Manager system, the system displays the **Ongoing** conference page and they have access to the following menu items:

**Device Administrator Role, Responsibilities, and Menus**

The Device Administrator role is for those users who administrate endpoints, bridges, and other network devices. For the areas to which they belong, users assigned the Device Administrator role can:

- Monitor endpoints, peripherals, and network devices.
- Add, edit, and delete endpoints and network devices.
- Provision endpoints.
- Update endpoints.
Add, edit, and delete rooms.

When device administrators log into the RealPresence Resource Manager system, the system displays the system Dashboard and they have access to the following menu items:

- **Auditor Role, Responsibilities, and Menus**

  The **Auditor** role allows security-conscious companies to separate system administration functions from system auditing functions. This provides an added level of system checks and balances. This role must be explicitly assigned by an administrator.

  For the areas to which they belong, users assigned the **Auditor** role can:
  - View audit logs.
  - Backup and delete audit logs.
  - Change the audit log file alert level.
  - Generate online Endpoint Usage Reports.
  - View and download system log files.
  - Respond to audit log alerts.

  When auditors log into the RealPresence Resource Manager system, the system displays the **Audit Log Files** page and they have access to the following menu items:
Administrator Role, Responsibilities, and Menus

The Administrator role is for those users who administrate the RealPresence Resource Manager system itself. Users assigned the Administrator role can generally do almost all system functions, however they cannot schedule conferences, monitor conferences, or manage endpoints or other network devices.

When administrators log into the RealPresence Resource Manager system, the system displays the system Dashboard and they have access to the following menu items:

- Conference
  - Future
  - Ongoing
  - Anytime

- Section
  - Monitor View
  - Peripherals View
  - Bundled Provisioning
  - Automatic Provisioning
  - Scheduled Provisioning
  - Automatic Software Update
  - Scheduled Software Update

- Network Device
  - Monitor View
  - VPBs
  - SBCs
  - MCUs
  - DMA
  - DMA Pool Orders
  - Access Control Servers

- User
  - Users
  - Groups
  - User Roles
  - Guest Book
  - Favorites

- Reports
  - Site Statistics
  - Site-Link Statistics
  - Endpoint Usage Report
  - Conference Usage Report
  - Conference Type Report
  - System Log Files
  - Audit Log Files

Admin
- Dashboard
- Conference Templates
- Conference Settings
- Provisioning Profiles
  - Automatic Provisioning Profiles
  - Scheduled Provisioning Profiles
- Software Updates
  - Automatic Software Updates
  - Scheduled Software Updates
- Rooms
- Areas
- Area Logs
- Directories
- Server Settings
  - Network
  - System Time
  - Database
- Calendaring Management
  - Licenses
  - Redundant Configuration
  - System Logs
  - Remote Alert Setup
  - Email
  - SNMP Settings

Admin (continued)
- Management and Security
  - Server Software Upgrade
  - Certificate Management
  - Session Management
  - Endpoint Management Settings
  - Local User Account Config
  - Local Password Requirements
  - Machine Accounts
  - Database Security

- Topology
  - Site Topology
  - Sites
  - Site Links
  - Site-to-Site Exclusions
  - Network Clouds
  - Territories

- Alert Settings
  - CMA Alert Level Settings
  - Endpoint Alert Level Settings
  - Remote Alert Profiles
  - Backup System Settings
  - Upgrades
  - Troubleshooting Utilities
  - Report Administration

Customized Roles and Responsibilities

The RealPresence Resource Manager system allows you almost unlimited flexibility in defining and redefining roles, but for simplicity and clarity, we recommend keeping the default roles with their default permissions and responsibilities.

Users can be assigned multiple roles and permissions are cumulative, so your business can combine roles as needed to reflect the workload your people undertake to manage and use the system.
Managing Users

This chapter includes information on managing users and groups within the Polycom® Real Presence® Resource Manager system. It includes these topics:

• “Manage Users” on page 277
• “Manage Groups” on page 289
• “Manage User Roles” on page 291
• “Manage System Guest Book” on page 296
• “Manage Favorites” on page 301

Manage Users

In the RealPresence Resource Manager system, only users assigned the Administrator role can manage users. Some of these tasks include:

• “Search for a User” on page 278
• “Add a Local User” on page 279
• “Edit a User” on page 281
• “View Role Information for a User” on page 282
• “Delete a User” on page 283
• “Unlock a User Account” on page 283
• “Import Users” on page 284
• “Updating Users by Import” on page 287
Search for a User

To search for a user
1. Go to User > Users and in the Search Users field, enter the name of the user of interest.

Searches for a user are case-insensitive, prefix searches of the Username, First Name, and Last Name fields.

2. To search for a local user, press Enter.
3. To search both local and enterprise users, first clear the Local Users Only check box and then press Enter.

If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

The first 500 users in the database that match your search criteria are displayed in the Users list.

4. If the list is too large to scan, further refine your search string.

View User Information

You can view information about a user, local or enterprise.

To view the address book a user is assigned to
1. Go to User > Users.
2. Select the user you want.
3. Click View Details.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td>The user’s first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The user’s last name.</td>
</tr>
<tr>
<td>User ID</td>
<td>The user’s unique login name. This user ID must be unique across all rooms</td>
</tr>
<tr>
<td></td>
<td>and users and across all domains.</td>
</tr>
</tbody>
</table>
To add a local user

1. Go to **User > Users** and click **Add**.

   The **Add New User** dialog box appears. The **Enable User** option is selected by default.

2. Enter the following user information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>The user’s first name</td>
</tr>
<tr>
<td>Last Name</td>
<td>The user’s last name</td>
</tr>
</tbody>
</table>
In the **Associated Endpoints** section, select and move the required endpoints(s) to **Selected Endpoints** list. Move the unwanted endpoints(s) to the **Available Endpoints** list. Press **Shift-click** or **Ctrl-click** to select multiple items in the list.

In the **Associated Roles** section, select and move the required role(s) to **Selected Roles** list. Move the unwanted role(s) to the **Available Roles** list. Press **Shift-click** or **Ctrl-click** to select multiple items in the list.

If the user has multiple endpoints, list the endpoints in order of priority, with the primary endpoint first.

If Areas are enabled, click the **Managed Areas** section.

You must have either the administrator role or have the area administrator role and be allowed to manage more than one area in order to perform this action.
— If the user has not been assigned a role, select the **None** radio button and continue to the **Associated Alert Profile** section.

— If the user has been assigned a role, select the **Specific Areas** radio button.

6 In the **Available Areas** section, select and move the required area(s) to **Selected Areas** list. Move the unwanted role(s) to the **Available Areas** list. Press **Shift-click** or **Ctrl-click** to select multiple items in the list.

The user will be assigned to manage the areas in the **Selected Areas** section.

7 In the **Associated Alert Profile** section, select a **Remote Alert Notification Profile** as appropriate.

8 In the **Dial String Reservations** section, select the user’s **endpoint** and enter the appropriate dial strings for **SIP URI**, **E164**, and **H323 ID**, then click **Apply**.

The dial strings appear in the list below.

If the user has multiple endpoints, enter the dial strings for one endpoint type at a time and click **Apply** each time.

9 Click **OK**.

If the **Phone Number** you entered is exactly the same as an existing user or endpoint, the **Phone Number Conflict** dialog box appears and lists the names of the other users or endpoints with the same number.

— To keep the duplicate number, click **Continue**.
— To change the phone number, click **Cancel**.

### Edit a User

For local users added manually to the RealPresence Resource Manager system, you can edit all user information. If you change the user ID, the user must log into the associated endpoints with the new ID.

For users added through the enterprise directory, you can edit their roles (unless the role is inherited from a group) and associate them to endpoints, but you cannot change user names, user IDs, or passwords.

#### To edit a user

1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.
2 To search for a local user, press Enter.

3 To search both local and enterprise users, first clear the Local Users Only check box and then press Enter.

If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

4 If the list is too large to scan, further refine your search string.

5 Select the user of interest and click Edit.

6 As required, edit the General Info, Associated Devices, Associated Roles, Managed Areas, Associated Alert Profile, and Dial String Reservations sections of the Edit User dialog box.

7 Click OK.

View Role Information for a User

A user with the Administrator role or Area Administrator role can view role information for a user.

To view permissions a user

1 Go to User > Users and in the Search Users field, enter the name of the user of interest.

Searches for a user are case-insensitive, prefix searches of the Username, First Name, and Last Name fields.

2 To search for a local user, press Enter.

3 To search both local and enterprise users, first clear the Local Users Only check box and then press Enter.

If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

4 If the list is too large to scan, further refine your search string.

5 Select the user of interest and click View Details.

The Edit User dialog box displays.

6 Click Associated Roles to view the role information for this user.
Delete a User

You can only delete local users from the RealPresence Resource Manager system. You cannot delete users added through integration with an enterprise directory.

To delete a user

1. Go to User > Users and in the Search Users field, enter the name of the user of interest.
2. To search for a local user, press Enter.
3. To search both local and enterprise users, first clear the Local Users Only check box and then press Enter.
4. If the list is too large to scan, further refine your search string.
5. Select the user of interest and click Delete.
6. Click Yes to confirm the deletion.

The user is deleted from the Resource Manager system.

Unlock a User Account

When a local user reaches the Failed login threshold, the system will not allow the user to log in until an administrator unlocks the user’s account. When a user’s account is locked, the system will display an error message.

To unlock a user account

1. Go to User > Users and in the Search Users field, enter the name of the user of interest and press Enter.
2. Select the user of interest and click Edit.
3 Enable the **Unlock User** option and click **OK**.

The system should allow the user to log in.

**Import Users**

You can import users into your RealPresence Resource Manager system. You may choose to do this if your RealPresence Resource Manager deployment does not include an integration with an LDAP server and you need the convenience of importing users in bulk instead of creating them one at a time.

### Importing Users When Areas Are Enabled

You can only import users to one area at a time and must have either the administrator role or area administrator role in order to import users.

### To import users to your system,

1. “Create a CSV File Containing the User Information you need” on page 284.
2. “Import the CSV File” on page 286.
3. “Review the Import Details File” on page 286.

### Create a CSV File Containing the User Information you need

You must create a CSV (comma separated values) file that contains the users you need. You can create this file with any plain text editor or use Microsoft Excel. The format should be the following:

Username, First Name, Last Name, Email, Title, Dept, City, Phone Number, Role(s), Password

Use the following guidelines:

- Use a file with a *.csv extension.
- All fields for a single user must be on a single line and end with a new line or end of file character. The line after a new line is assumed to be for another user.
- All fields for a single user must be on a single line and end with a new line or end of file character. The line after a new line is assumed to be for another user.
- Commas (’,’) are used as field separators and cannot be embedded in a field. All commas must be included, even before fields that are optional. Each field’s leading and trailing white space (blanks and tabs) is ignored (does not become part of the field value).
- Unicode characters are allowed in the file as long as they are valid for the field type.
• Blank lines are allowed and are ignored.
• A header line is not allowed in the CSV file. All lines must either represent a user or be blank.
• The following fields are required: **Username**, **First Name** or **Last Name**, and **Email**.
• Other fields can be left blank, but not skipped.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username must be unique across the entire RealPresence Resource Manager system. (The recommended naming convention to ensure uniqueness is specified in section If a specified username already exists in the selected area (or in the system, if Areas is disabled), then the system assumes you wish to update the existing user's information. If a specified username already exists in a different area, then the user is neither added nor updated and an error is issued.</td>
</tr>
<tr>
<td>Role(s)</td>
<td>Role names are case sensitive. To specify multiple roles for a user, separate the roles with a pipe ('</td>
</tr>
<tr>
<td>Password</td>
<td>If any of the users have no password specified, then a single default password is generated and assigned to all those without a password specified. The administrator will be shown what password was assigned to all and is responsible for writing it down and communicating it to all the users. For users assigned default passwords, the first time they log in, they will be required to change their password.</td>
</tr>
<tr>
<td>Email</td>
<td>Be sure to includes a valid email address.</td>
</tr>
</tbody>
</table>

**Examples**

This first example shows all fields specified:

```
js@co.com, John, Smith, js@co.com, Tech I, IT, Boulder, 303-333-4444, Role 1|Role 2, JSpw
```

This example shows only the required fields specified. In this case, the user will be given a blank first name, title, department, city and phone number, no role and a generated password.

```
jdoe, , Doe, doe@co.com, , , ,scheduler, ,
```
**Import the CSV File**

You need to have either an administrator or area administrator role to import users.

**To import local users to the RealPresence Resource Manager system**

1. Choose User > Users and click Import Local Users.
2. In the File Location (CSV) field, browse to the location of the CSV file you created.
3. If areas are enabled and you manage more than one area, select an area from the Assign Area drop-down list.
4. Click Import. A status window appears. Click OK when it is complete.
5. The results of the import are summarized on the Import Summary screen.
6. If a default password is shown in the summary, write the password down and inform those users of the password.
7. Click Download Import Details to view the import details file. Save it as a text file for your records.
8. Close the Import Users dialog box.

**Importing Users into an Area**

If Areas are not enabled on your RealPresence Resource Manager system or you only manage one area, the Areas drop-down is not available.

If Areas are enabled and you manage more than one area, you must select an area to which all the users will be added. You can also select None to add the users to no area.

4. Click Import.

   A status window appears. Click OK when it is complete.

   The results of the import are summarized on the Import Summary screen.

5. If a default password is shown in the summary, write the password down and inform those users of the password.

**Default Passwords Created During Import**

If you fail to record/remember the password shown on the Import Summary screen, there will be no other way to determine it and the users will be unable to login. If this happens, you can either:

- Edit each affected user one-by-one via the RealPresence Resource Manager system’s User Edit screen and manually change the password field or have the system generate a password.
- Delete all affected users one-by-one via the RealPresence Resource Manager user interface and re-import them.

6. Click Download Import Details to view the import details file. Save it as a text file for your records.

7. Close the Import Users dialog box.

**Review the Import Details File**

You should review the Import Details file for any information about errors that may need to be corrected.
If there are errors, you can either:

- **Create another CSV file** with the users that need to be corrected and import only those users.
- **Edit the same CSV file** to correct the users with errors and import the file again. Users that were previously added successfully will be updated, see “Updating Users by Import” on page 287. Specifically, existing user updates will fail if a password is specified, so either remove those user’s passwords or ignore password errors that are issued for those users who were previously added.

In either case, realize that a different default password will be assigned in subsequent imports than was assigned to users in a previous import.

If there are errors and you do not view the Import Details file, you will not know what errors were issued or for which users.

### Updating Users by Import

You can also use the Import Local Users action to update existing users.

The CSV format for updating an existing user is the same as that used for adding a user except that the password field must be blank. For each existing username whose attributes are to be updated, the CSV format is:

**Username, First Name, Last Name, Email, Title, Dept, City, Phone Number, Role(s),**

Note that the comma after the Role(s) field is still required.

Importing a CSV file that has existing usernames will overwrite existing data. Make sure the CSV data is at least as current as what is in RealPresence Resource Manager system. Determining existing user data can be done one-by-one and manually via the RealPresence Resource Manager system user interface (currently there is no way to export local user data in bulk).

A single CSV file may contain both users to be added and users to be updated. The system will automatically determine whether you are intending to add or update a user by whether the username already exists in the system or not:

The following fields cannot be changed using the Import Local Users action.

- An existing user’s username
- An existing user’s password
- Any of the attributes not specified in the Import CSV format

The following rules apply when updating existing users.
• The Username must already exist in the selected area. You can only change an existing user’s username by using the Resource Manager system user interface.

• The Password must be blank. If a password is specified, the update for that user will fail such that none of the fields will be updated. You cannot change a user’s password with an import. You must use the system’s web interface.

• Fields that are left blank will replace any existing data that the Resource Manager system has for that user with a blank.

• There is no way to indicate that any of the user’s data should be left as is.

• All other user attributes not included in the CSV format, such as which areas a user manages, will not be modified by an Import.
Manage Groups

In the RealPresence Resource Manager system, only users assigned the Administrator role can:

- “Add a Local Group” on page 289
- “Import Enterprise Groups” on page 290
- “Edit a Group” on page 291
- “Delete a Group” on page 291

Add a Local Group

To add a local group

1. Go to User > Groups.
2. In the Groups page, click Add Local Group.
3. Complete the General Info section of the Add Local Group dialog box.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td></td>
</tr>
<tr>
<td>Group Name</td>
<td>A meaningful and unique group name assigned when creating the group.</td>
</tr>
<tr>
<td>Description</td>
<td>A more complete description of the group’s purpose</td>
</tr>
<tr>
<td>Directory Viewable</td>
<td>Whether or not the group is displayed in the endpoint directory</td>
</tr>
<tr>
<td>Provisioning Profile</td>
<td>The automatic provisioning profile assigned when creating the group.</td>
</tr>
<tr>
<td>Address Book</td>
<td>See “Assign Address Books to Groups” on page 392.</td>
</tr>
<tr>
<td>Assigned Area</td>
<td>If your RealPresence Resource Manager system has areas enabled, you can choose to assign this user to an area that you manage.</td>
</tr>
</tbody>
</table>

Associated Roles

| Available Roles | The list of roles defined to the RealPresence Resource Manager system.     |
| Selected Roles  | The list of roles that you assign users when adding them to the system. Users have all of the permissions associated with all of the roles assigned to them (that is, permissions are cumulative). |
In the **Search Available Members** field of the **Group Members** dialog box, search for the users and groups to add to this local group.

In the **Search Results** section, select and move the users and groups of interest to the **Group Members** list. To select all users and groups listed, click the check box in the column header.

Click **OK**.

The group appears in the **Groups** list. It is identified as a LOCAL group.

## Import Enterprise Groups

**To import one or more enterprise groups**

1. Go to User > Groups.
2. In the **Groups** page, click **Import Enterprise Group**.
3. In the **Search Available Groups** field of the **Import Enterprise Group** dialog box, type all or part of the group name (with wildcards) and press **ENTER**.

Searches for a group are case-insensitive, exact-match searches of the **Group Name** field. Use wildcard characters to perform substring searches.

4. In the **Search Results** list, select the enterprise groups to add. To select all enterprise groups, click the check box in the column header.
5. Click the right arrow to add the enterprise groups to the **Groups to Import** list.
6. Click **OK**.

The enterprise group appears in the **Groups** list. Now you can edit the group and associate it with an automatic provisioning profile, user roles, and specify whether or not the group directory is viewable. You can also search for enterprise users.
Edit a Group

To edit a local or enterprise group
1 Go to User > Groups.
2 In the Groups page, select the group of interest and click Edit.
3 As required, edit the General Info, Associated Roles, and Group Members sections of the Edit Local Groups dialog box.

- The Group Members section is only available for Local groups.
- If you remove a user from a group or a role from a group, the user no longer has the roles associated with the group.

4 Click OK.

Delete a Group

To delete a local or enterprise group
1 Go to User > Groups.
2 In the Groups page, select the group of interest and click Delete Group.
3 Click Yes to confirm the deletion.
   The group is deleted from the system.

An enterprise group is only deleted from the system, not the enterprise directory, so it can be re-imported.

Manage User Roles

In the RealPresence Resource Manager system, only users assigned the Administrator role can:

- “Assign Users Roles and Endpoints” on page 292
- “View the List of User Roles” on page 292
- “Add a User Role” on page 293
- “Edit Permissions for a User Role” on page 294
- “Delete a User Role” on page 294
Assign Users Roles and Endpoints

You can assign roles to both local and enterprise users and associate them with endpoints.

To assign a role and endpoint to a user

1. Go to User > Users.
2. To search for a user:
   a. In the Search field of the Users page, type a search string.
   b. To search both local and enterprise users, clear the Local Users Only check box and press Enter.
      The first 500 users in the database that match your search criteria are displayed in the Users list.
   c. If the list is too large to scan, further refine your search string.
3. Select the user of interest and click Edit.
4. In the Devices section of the Edit User dialog box, select the endpoint to associate with the user and move it to the Selected Devices column. If a user has multiple endpoints, the first endpoint listed is the user’s default endpoint.
5. In the Associated Roles section, select and move the required role(s) to Selected Roles list. Move the unwanted role(s) to the Available Roles list. Press Shift-click or Ctrl-click to select multiple items in the list.
6. Click Finish.

View the List of User Roles

To view the list of User Roles

Go to User > User Roles.

The User Roles list appears. It can be filtered by Name and Description.
Add a User Role

When you add a user role, you also specify permissions for the role.

To add a new user role

1. Go to User > User Roles.
2. On the User Roles page, click Add.
3. Complete the Name and Description fields of the Add Role dialog box and assign permissions to the new role.

The following table describes the fields of the Add Role dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name (ASCII only) of the user role</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A useful description (ASCII only) of the user role</td>
</tr>
<tr>
<td>Administrator</td>
<td>Identifies which RealPresence Resource Manager system administrator pages and functions are available to the user role.</td>
</tr>
<tr>
<td>Operator Permissions</td>
<td>Identifies which RealPresence Resource Manager system operator pages and functions are available to the user role.</td>
</tr>
<tr>
<td>Scheduler Permissions</td>
<td>Identifies which RealPresence Resource Manager system scheduling pages and functions are available to the user role.</td>
</tr>
<tr>
<td>Scheduling Level</td>
<td></td>
</tr>
<tr>
<td>Basic</td>
<td>Users can schedule conferences using the conference templates defined for them. They cannot access or edit the advanced Conference Settings.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Users can schedule conferences using the conference templates defined for them. They can also access and edit the advanced Conference Settings.</td>
</tr>
</tbody>
</table>

4. Click Save.

The new user role appears in the RealPresence Resource Manager system.
**Edit Permissions for a User Role**

You can change permissions for the default roles, as well as for other user roles that were created manually. You cannot change permissions for the default Administrator role.

**To edit the permissions for a user role**

1. Go to User > User Roles.
2. As needed, use the Filter to customize the User Roles list.
3. In the User Roles list, select the role of interest and click Edit.
4. Edit the Description field of the Edit Role dialog box and edit permissions for the role.
5. Click Save.

**Delete a User Role**

You can delete a user role from the RealPresence Resource Manager system, provided no users are currently assigned to it.

**To delete a user role**

1. Go to User > User Roles.
2. As needed, use the Filter to customize the User Roles list.
3. In the User Roles list, select the role of interest and click Delete.
4. Click Yes to confirm the deletion.

   The user role is deleted from the RealPresence Resource Manager system.

**View the Groups and Users Associated with a User Role**

**To view which groups and users are associated with a specific user role**

1. Go to User > User Roles.
2. As needed, use the Filter to customize the User Roles list.
3. In the User Roles list, select the role of interest and click View Associated Groups and Users.

   The View Associated Groups and Users dialog box appears.
**Assign Users to Manage an Area(s)**

This task is only available if areas have been enabled (multi-tenancy).

In order to perform RealPresence Resource Manager tasks within an area, the user must be allowed to manage that area. Allowing a user to manage an area means allowing them to perform the duties associated with their role in the areas that they are allowed to manage.

A user can be allowed to manage:

- **Zero areas.** This means that user cannot perform any tasks in any area.
- **One Area.** This means that the user can perform role-based tasks for the area he manages. You must indicate which area you want the user to manage.
- **Multiple areas.** This means the user can perform role-based tasks in each area that he manages. You must indicate which areas you want the user to manage.
- **All areas.** A user can manage all areas if he is assigned a system role or if his role includes the View and/or Modify All areas permission. If the user has this role, you do not need to explicitly allow him to manage an area or areas.

For example, a user with the area scheduler role can belong to the yellow area and allowed to schedule conferences in both the yellow and blue areas if he has permission to manage the blue area as well as the yellow area.

In order to enable a user to manage an area, you must have the administrator role or the area administrator role and manage the area to which you want to allow a user to manage. In short, you need to have permission to manage the area to which you want to allow a user to manage.

**To assign a user to manage an area(s)**

1. Go to User > Users.
2. Enter the name for the user of interest in the Search Users field and press Enter.

   Searches for a user are case-insensitive, prefix searches of the Username, FirstName, and Last Name fields.

3. Select the user to assign to an area and choose the Edit action.
4. In the Edit User dialog, click Managed Areas.

   You must have either the administrator role or have the area administrator role and be allowed to manage more than one area in order to perform this action.
5 Select the **Specific Areas** radio button.

6 In the **Available Areas** section, mark the area(s) you want the user to manage and click the arrow icon to move the list to the **Selected Areas** section.

   Conversely, you can mark area(s) in the **Selected Areas** section and click the corresponding arrow to move the marked area(s) to the **Available Areas** section.

   The user will be assigned to manage the areas in the **Selected Areas** section.

7 Click **OK**.

---

### Manage System Guest Book

The Guest Book provides a way to store conference participants that aren’t managed by the RealPresence Resource Manager system.

It includes these topics:

- “Guest Book Considerations for Multi-Tenancy” on page 296
- “User Menu and Guest Book” on page 296
- “Context-Sensitive Guest Book Actions” on page 297
- “Add a Guest to the System Guest Book” on page 297
- “Edit a Guest in the System Guest Book” on page 300
- “Delete a Guest from the System Guest Book” on page 300

### Guest Book Considerations for Multi-Tenancy

When areas are enabled for your system, area users can view only those guests who have been assigned to an area that they manage. If a user can manage more than one area, he can view users from all areas that he manages. For more information, see “Area Conference Guests” on page 402.

### User Menu and Guest Book

By default, both system and area schedulers, operator, and administrators have access to the **User Menu** and **Guest Book**.

The **Guest Book** is a local system directory that includes guest participants who were either:

- Explicitly added to the **Guest Book**.
- Saved to the **Guest Book** while being added as conference participants.
They are referred to as static entries because they are not imported through the dynamically updated enterprise directory or included in the system Global Address Book. The Guest Book is limited to 500 entries. The Guest Book has these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The guest’s first and last name.</td>
</tr>
<tr>
<td>Email</td>
<td>The guest’s E-mail address. The system validates the E-mail structure only.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the guest's endpoint system. This is a free-form entry field</td>
</tr>
<tr>
<td>Number</td>
<td>(Optional) The ISDN phone number for the user. This number is constructed</td>
</tr>
<tr>
<td></td>
<td>from the Country code + Area/City code + phone number or entered as the</td>
</tr>
<tr>
<td></td>
<td>modified dial number.</td>
</tr>
<tr>
<td>Join Mode</td>
<td>Indicates whether the guest will use an audio endpoint or video endpoint</td>
</tr>
<tr>
<td></td>
<td>to join conferences.</td>
</tr>
<tr>
<td>Dial Options</td>
<td>Indicates whether the guest will dial into conferences or that the system</td>
</tr>
<tr>
<td></td>
<td>should dial out to the guest.</td>
</tr>
<tr>
<td>Dial Type</td>
<td>Indicates whether the guest has an H.323 (IP), SIP (IP), or H.320 (ISDN)</td>
</tr>
<tr>
<td></td>
<td>endpoint.</td>
</tr>
<tr>
<td>Selected Area</td>
<td>This field is available when areas are enabled and the user can manage</td>
</tr>
<tr>
<td></td>
<td>more than one area.</td>
</tr>
</tbody>
</table>

Context-Sensitive Guest Book Actions

The Actions section of the Guest Book page may include these context-sensitive actions depending on what is selected.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Guest</td>
<td>Use this command to add a new guest user.</td>
</tr>
<tr>
<td>Edit Guest</td>
<td>Use this command to change information for a guest user.</td>
</tr>
<tr>
<td>Delete Guest</td>
<td>Use this command to delete a guest from the Guest Book. Deleting a guest</td>
</tr>
<tr>
<td></td>
<td>is a permanent operation.</td>
</tr>
</tbody>
</table>

Add a Guest to the System Guest Book

To add a guest to the system Guest Book

1. Go to User > Guest Book and click Add Guest.
2 Configure the **Guest Information** section of the **Add New Guest** dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>The guest's first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>The guest's last name.</td>
</tr>
<tr>
<td>Email</td>
<td>The guest's E-mail address. The system only validates the structure of the E-mail address.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the guest's endpoint system. This is a free-form field that the system does not validate.</td>
</tr>
<tr>
<td>Dial Type</td>
<td>Specify the protocol that the guest's endpoint supports: H.323 (IP), SIP (IP), or H.320 (ISDN). This selection will determine what other sections of the <strong>Add New Guest</strong> dialog box you will need to complete.</td>
</tr>
<tr>
<td>Join Mode</td>
<td>Specify whether the guest's endpoint is an audio or video endpoint.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>A guest may have multiple endpoints. Create a separate <strong>Guest Book</strong> entry for each endpoint.</td>
</tr>
<tr>
<td>Dial Options</td>
<td>Specify whether the guest will dial into conferences, or require that the system dial out to the guest.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>To support both options, create a separate <strong>Guest Book</strong> entry for each.</td>
</tr>
<tr>
<td>Assigned Area</td>
<td>This field is available when areas are enabled and the user can manage more than one area.</td>
</tr>
</tbody>
</table>

3 If the guest has an H.323 (IP) endpoint, configure these settings:
If the guest has a SIP (IP) endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Number and Number Type     | The specific dial string for the guest, and the format of the number that the MCU must resolve to contact the guest. This may be an IP address, E.164 address, H.323, or Annex-O. For Annex-O dialing, in the **Number** field enter the H.323.alias@IP, for example:  
  - 1001@11.12.13.14  
  - 1001@domain.com  
  - username@domain.com  
  - username@11.12.13.14  |
| **Notes**                  | • Polycom endpoints must register with a gatekeeper before they will attempt an Annex-O call.  
  • You can enter a dial string for another MCU as a guest. If so, you may need to specify the conference ID in the **Extension** field also. |
| Extension                  | Use this field to connect the conference to another conference on another MCU. In this field, specify the conference ID or passcode for the conference on the other MCU. |
| MCU Service                | Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at **Any Available Service** unless you have specific knowledge of MCU services. |

4 If the guest has a SIP (IP) endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sip URI</td>
<td>The SPI URI the MCU must resolve to contact the guest.</td>
</tr>
<tr>
<td>MCU Service</td>
<td>Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at <strong>Any Available Service</strong> unless you have specific knowledge of MCU services.</td>
</tr>
</tbody>
</table>
If the guest has an H.320 (ISDN) endpoint, configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Modified Dial Number</td>
<td>Select this option first (as needed) as it will determine the other fields you must configure.</td>
</tr>
<tr>
<td>Country</td>
<td>(Not available when Use Modified Dial Number is selected.) The country to which the system will dial out to the guest. Click Select to view a list of country codes.</td>
</tr>
<tr>
<td>Area/City Code</td>
<td>(Not available when Use Modified Dial Number is selected.) The area code to which the system will dial out to the guest.</td>
</tr>
<tr>
<td>Number</td>
<td>The participant’s phone number.</td>
</tr>
<tr>
<td>Extension</td>
<td>Cannot be configured.</td>
</tr>
<tr>
<td>MCU Service</td>
<td>Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system has registered. Leave this at Any Available Service unless you have specific knowledge of MCU services.</td>
</tr>
</tbody>
</table>

6 Click OK.

**Edit a Guest in the System Guest Book**

**To edit a guest in the system Guest Book**

1 Go to User > Guest Book and select the guest of interest.
2 Click Edit Guest.
3 Change the Guest Information section and endpoint information sections of the Add New Guest dialog box, as needed. For more information about these fields, see “Add a Guest to the System Guest Book” on page 297.
4 Click OK.

**Delete a Guest from the System Guest Book**

**To delete a guest from the system Guest Book**

1 Go to User > Guest Book and select the guest of interest.
2 Click Delete Guest.
3 Click Yes to confirm the deletion.

**Manage Favorites**

The RealPresence Resource Manager system allows users with the operator role or area operator role to create one or more Favorites list, which they can use to quickly select participants to participate in conferences.

The operations associated with managing favorites include:

- “Add a Favorites List” on page 301
- “Edit a Favorites List” on page 302
- “Delete a Favorites List” on page 302

In the RealPresence Resource Manager system, only users with the operator or area operator roles with Monitoring permissions can view, add, edit, delete, or use Favorites lists and these Favorites lists cannot be shared with other operators.

**Add a Favorites List**

**To add a Favorites list**

1 Go to User > Favorites.
2 On the Favorites page, click Add.
3 Complete the Favorites List Name and Description fields of the Add Favorites List dialog box.

The Favorites List Name must be unique within the system.

4 In the Search Available Members field enter all or part of the person’s last name or first name and click Search.

The system searches the Users list (local and domain) for users who are associated with endpoints and who meet your search criteria. The results appear in the Search Results column.

- Depending on the search domain, the search function may return different results. See Filter and Search a List.
- The search results only include users associated with endpoints.
Select the user(s) of interest from the list and move them to the Favorite List Members column.

Repeat step 4 and 5 until you’ve added the users of interest to your Favorites list and then click OK.

The new list appears in the Favorites page.

## Edit a Favorites List

### To edit a Favorites list

1. Go to User > Favorites.
2. On the Favorites page, select the Favorites list of interest and click Edit.
3. In the Edit Favorites List dialog box, edit the Favorites List Name and Description fields as needed.
4. Remove or add users to the Favorite List Members column as needed and then click OK.

## Delete a Favorites List

### To delete a Favorites list

1. Go to User > Favorites.
2. On the Favorites page, select the Favorites list of interest and click Delete.
3. Click Yes to confirm the deletion.

   The list is deleted from the RealPresence Resource Manager system.
This chapter describes the reports available through the Polycom® RealPresence® Resource Manager system and how to view and export them. Use these reports to identify return on investment, troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls. It includes these topics:

- “Report Considerations for Multi-Tenancy” on page 303
- “Site Statistics Report” on page 303
- “Site Link Statistics Report” on page 305
- “Endpoint Usage Report” on page 307
- “Conference Usage Report” on page 313
- “Conference Type Report” on page 313
- “View and Export System Log Files” on page 316
- “Download Log Files” on page 317
- “View and Download Audit Log Files” on page 317
- “Resource Manager System Report” on page 318

Report Considerations for Multi-Tenancy

Area-specific information displays in reports when you have either the administrator role or the area administrator role AND can manage more than one area.

Site Statistics Report

Use the Site Statistics report to check call rate and call quality statistics for the sites. You can view the data in a grid or graphically.
To view Site Statistics

1. Go to Reports > Site Statistics.

The Site Statistics appear with the statistics displayed in a grid. The grid shows a snapshot of the current statistics. The data is updated automatically every 15 seconds.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>Specifies the site to which the statistics apply.</td>
</tr>
<tr>
<td>Num of Calls</td>
<td>Specifies the number of currently active calls for the site.</td>
</tr>
<tr>
<td>% Bandwidth Used</td>
<td>Specifies the cumulative bandwidth used by the currently active calls.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td></td>
</tr>
<tr>
<td>Avg Bit Rate</td>
<td>Specifies the average bit rate for the currently active calls that is, the total bit rate for all currently active calls divided by the number of active calls.</td>
</tr>
<tr>
<td>% Packet Loss</td>
<td>Specifies the average percentage of packet loss for the currently active calls that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.</td>
</tr>
<tr>
<td>Avg Jitter</td>
<td>Specifies the average jitter for the currently active calls that is, the total jitter for all currently active calls divided by the number of active calls.</td>
</tr>
<tr>
<td>Avg Delay</td>
<td>Specifies the average delay for the currently active calls that is, the total delay for all currently active calls divided by the number of active calls.</td>
</tr>
</tbody>
</table>

2. To view the Site Statistics graphically and over a selected period of time:
   a. Click View Chart.
   b. In the Site Name list, select the site(s) to chart.
   c. In the Y-Axis list, select the statistic(s) to chart.
   d. In the Data Limit field, enter the time frame in minutes for which to chart the data. The default is 60 minutes.

   The charts are dynamically updated for your selections.
Site Link Statistics Report

Use the Site Link Statistics report to check call rate and call quality statistics for all site links. You can view the data in a grid or graphically.

To view Site Link Statistics

1. Go to Reports > Site Link Statistics.

The Site Link Statistics appear with the statistics displayed in a grid. The grid shows a snapshot of the current statistics. The data is updated automatically every 15 seconds.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Link Name</td>
<td>Specifies the two linked sites for which the statistics apply.</td>
</tr>
<tr>
<td>Num of Calls</td>
<td>Specifies the number of currently active calls for the site link.</td>
</tr>
<tr>
<td>% Bandwidth Used</td>
<td>Specifies the percentage of bandwidth used by the currently active calls, that is, the bandwidth used by the currently active calls divided by the total available bandwidth for the link expressed as a percentage.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Specifies the total bandwidth of the link.</td>
</tr>
<tr>
<td>Avg Bit Rate</td>
<td>Specifies the average bit rate for the currently active calls, that is, the total bit rate for all currently active calls divided by the number of active calls.</td>
</tr>
<tr>
<td>% Packet Loss</td>
<td>Specifies the average percentage of packet loss for the currently active calls that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.</td>
</tr>
<tr>
<td>Avg Jitter</td>
<td>Specifies the average jitter for the currently active calls that is, the total jitter for all currently active calls divided by the number of active calls.</td>
</tr>
<tr>
<td>Avg Delay</td>
<td>Specifies the average delay for the currently active calls that is, the total delay for all currently active calls divided by the number of active calls.</td>
</tr>
</tbody>
</table>

2. To view the Site Link Statistics graphically:
   a. Click View Chart.
   b. In the Site Name list, select the site(s) to chart.
   c. In the Y-Axis list, select the statistic(s) to chart.
Call Detail Record Report Administration

By default, the RealPresence Resource Manager system stores the conference and endpoint call detail records (CDRs) for 30 days. You can modify the CDR retention period and you can schedule a weekly archive of the CDRs. These procedures are described in the following topics.

Modify the CDR Retention Period

By default, the conference and endpoint CDRs are purged after 30 days.

To change how long CDR information is retained

1. Go to Admin > Report Administration.
2. In the Report Administration page, enter the number of Days to keep Conference and Endpoint CDRs.
3. Click Save Settings.

Schedule Archives of the CDR Report

To schedule archives of CDR information

1. Go to Admin > Report Administration.
3. Configure these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Transfer Date</td>
<td>Set the date for the next CDR transfer.</td>
</tr>
<tr>
<td>Transfer Start Time</td>
<td>Set the start time of the next transfer and all subsequent transfers.</td>
</tr>
<tr>
<td>CDR Transmission Frequency (In Days)</td>
<td>Set the number of days between each transfer.</td>
</tr>
</tbody>
</table>
To verify that the FTP settings are functional, click **Test Archive Settings**.

When the settings are correct, click **Save Settings**.

## Endpoint Usage Report

The **Endpoint Usage Report** is based on the CDRs extracted from selected endpoints and includes entries for ISDN and IP calls. (Currently, the RealPresence Resource Manager system reports CDRs for the Polycom HDX Series, V and VSX Series, VVX, and CMA Desktop endpoints as well as supported TANDBERG and LifeSize endpoint models.)

Use data from the **Endpoint Usage Report** to troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls.

### To view the Endpoint Usage Report

1. Go to **Reports > Endpoint Usage Report**.

   The **Endpoint Usage Report** page appears displaying the following information for the endpoints for which CDRs are available.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>The registered serial number of the endpoint.</td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>The registered name of the endpoint.</td>
</tr>
</tbody>
</table>
The CDRs are displayed in alphabetical order for the default **Start Date** and **End Date**. By default, the CDRs for the last week are reported.

2. To restrict the report to a different time period, change the **Start Date** and **End Date**. The report is dynamically updated.

3. Use the **Filter** to customize the report by endpoint **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, **Site**, or **VIP** status.

   You can also filter on **Area** when areas are enabled and you manage more than one area.

4. To generate the Endpoint Usage report, select one or more endpoints to include in the report and click **Generate Report**. Use the **Ctrl** key to select multiple endpoints.

   The **Generate Report** page displays the **Summary** usage report for the selected endpoints. It includes the following information for the calls.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of calls</td>
<td>Specifies the number of calls the selected endpoints joined for the selected date range. Click <strong>Details</strong> to get more information about these calls.</td>
</tr>
<tr>
<td>Total call time</td>
<td>Specifies the total amount of time the selected endpoints spent in conference during the selected date range.</td>
</tr>
<tr>
<td>Average time per call</td>
<td>Specifies the average amount of time the selected endpoints spent in conference during the selected date range, that is, the total call time divided by the number of calls.</td>
</tr>
<tr>
<td>Average rate per call</td>
<td>Specifies the average bit rate for the selected calls.</td>
</tr>
</tbody>
</table>

   **Note**

   When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.

   **Owner/Room** The person or room to whom the endpoint is registered.

   **Area** Displays the area to which the endpoint is associated. This column only available when areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage. If you do not have permission to manage the area in which the endpoint belongs, the value in this column reads, “Restricted.”
5 To select a different group of endpoints, click **Change Selected**, select the endpoints, and click **Generate Report** again.

6 Click **Call Times** to see a chart that identifies the number of calls versus the start time for the calls.

7 Click **Inbound** to see a chart that identifies the endpoints from which the inbound calls to the selected endpoints originated.

8 Click **Outbound** to see a chart that identifies the endpoints to which the selected endpoints called.

9 Click **Summary CDR Report** to see a grid that displays information for each of the selected endpoints that participated in calls.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>The registered serial number of the endpoint.</td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>Identifies the endpoint by name.</td>
</tr>
<tr>
<td>Total Time in Call</td>
<td>Specifies the total amount of time the endpoint spent in conference during the selected time period.</td>
</tr>
<tr>
<td>Average Time in Call</td>
<td>Specifies the average amount of time the endpoint spent per call during the selected time period, that is, the <strong>Total Time in Call</strong> divided by the <strong>Total Calls</strong>.</td>
</tr>
<tr>
<td>Average Speed All Calls</td>
<td>Specifies the average bit rate for all of the calls in which the endpoint participated during the selected time period, that is, total bit rate divided by the <strong>Total Calls</strong>.</td>
</tr>
<tr>
<td>Calls Out</td>
<td>Specifies the number of calls in which the endpoint participated during the selected time period that originated from the endpoint.</td>
</tr>
<tr>
<td>Calls In</td>
<td>Specifies the number of calls in which the endpoint participated during the selected time period that did not originate from the endpoint.</td>
</tr>
<tr>
<td>Total Calls</td>
<td>Specifies the total number of calls in which the endpoint participated for the selected time period.</td>
</tr>
</tbody>
</table>

If any of the selected endpoints did not participate in calls during the selected time period, it is not included in the **Summary CDR Report**.

10 To export the information in the **Summary CDR Report**, click **Export as Excel File** and either **Open** or **Save** the file as needed. Note that only the first 1000 lines of the report are exported to the Excel file.

11 Click **Detail CDR Report** to see information for each of the endpoints that participated in calls.

The **Generate Report** page displays **System Information** and CDR information for the first endpoint in the list. For the selected endpoint, the **System Information** section includes the following data.
For each call from the selected endpoint, the CDR information includes the following data.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Information</td>
<td>Specifies the name of the selected endpoint.</td>
</tr>
<tr>
<td>Area</td>
<td>The area to which the endpoint is assigned. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.</td>
</tr>
<tr>
<td>Model</td>
<td>Specifies the model number of the selected endpoint.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies the IP address of the selected endpoint.</td>
</tr>
<tr>
<td>ISDN</td>
<td>Specifies the ISDN number or V.35 number.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Specifies the serial number of the selected endpoint.</td>
</tr>
<tr>
<td>Start Date Time</td>
<td>Specifies the start date and time for the conference.</td>
</tr>
<tr>
<td>End Date Time</td>
<td>Specifies the end date for the report. This also defaults to the current date.</td>
</tr>
<tr>
<td>Call Duration</td>
<td>Specifies how long the call lasted in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Account Number</td>
<td>If Require Account Number to Dial is enabled on the system, the value entered by the user is displayed in this field.</td>
</tr>
<tr>
<td>Remote System Name</td>
<td>Specifies the endpoint to which the endpoint was connected for the call.</td>
</tr>
<tr>
<td>Call Number 1</td>
<td>Specifies the IP or ISDN numbers for the endpoints to which the endpoint was connected for the call.</td>
</tr>
<tr>
<td>Call Number 2</td>
<td>Specifies the IP or ISDN numbers for the endpoints to which the endpoint was connected for the call.</td>
</tr>
<tr>
<td>Transport Type</td>
<td>The type of call — Either H.320 (ISDN), H.323 (IP), or SIP.</td>
</tr>
<tr>
<td>Call Rate</td>
<td>The bandwidth negotiated with the far site.</td>
</tr>
<tr>
<td>System Manufacturer</td>
<td>The name of the system manufacturer, model, and software version, if they can be determined.</td>
</tr>
<tr>
<td>Call Direction</td>
<td>In — For calls received. Out — For calls placed from the system.</td>
</tr>
<tr>
<td>Conference ID</td>
<td>A number given to each conference. A conference can include more than one far site, so there may be more than one row with the same conference ID.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call ID</td>
<td>Identifies individual calls within the same conference.</td>
</tr>
<tr>
<td>H.320 Channels</td>
<td>The total number of ISDN B channels used in the call. For example, a 384K call would use six B channels.</td>
</tr>
<tr>
<td>Endpoint Alias</td>
<td>The alias of the far site.</td>
</tr>
<tr>
<td>Endpoint Additional Alias</td>
<td>An additional alias of the far site.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>Terminal, gateway, or MCU.</td>
</tr>
<tr>
<td>Endpoint Transport Address</td>
<td>The actual address of the far site (not necessarily the address dialed).</td>
</tr>
<tr>
<td>Audio Protocol Tx</td>
<td>The audio protocol transmitted to the far site, such as G.728 or G.722.1.</td>
</tr>
<tr>
<td>Audio Protocol Rx</td>
<td>The audio protocol received from the far site, such as G.728 or G.722.</td>
</tr>
<tr>
<td>Video Protocol Tx</td>
<td>The video protocol transmitted to the far site, such as H.263 or H.264.</td>
</tr>
<tr>
<td>Video Protocol Rx</td>
<td>The video protocol received from the far site, such as H.261 or H.263.</td>
</tr>
<tr>
<td>Video Format Tx</td>
<td>The video format transmitted to the far site, such as CIF or SIF.</td>
</tr>
<tr>
<td>Video Format Rx</td>
<td>The video format received from the far site, such as CIF or SIF.</td>
</tr>
<tr>
<td>Disconnect Info</td>
<td>The description of the Q.850 (ISDN) cause code showing how the call ended.</td>
</tr>
<tr>
<td>Q850 Cause Code</td>
<td>The Q.850 cause code showing how the call ended.</td>
</tr>
<tr>
<td>Total H.320 Errors</td>
<td>The number of errors during an H.320 call.</td>
</tr>
<tr>
<td>Avg % Packet Loss Tx</td>
<td>The combined average of the percentage of both audio and video packets transmitted that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire H.323 call. However, it does report an average of the sampled values.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Avg % Packet Loss Rx</td>
<td>The combined average of the percentage of both audio and video packets received that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire H.323 call. However, it does report an average of the sampled values.</td>
</tr>
<tr>
<td>Avg Packet Loss Tx</td>
<td>The number of packets transmitted that were lost during an H.323 call.</td>
</tr>
<tr>
<td>Avg Packet Loss Rx</td>
<td>The number of packets from the far site that were lost during an H.323 call.</td>
</tr>
<tr>
<td>Avg Latency Tx</td>
<td>The average latency of packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Avg Latency Rx</td>
<td>The average latency of packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Max Latency Tx</td>
<td>The maximum latency for packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Max Latency Rx</td>
<td>The maximum latency for packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Avg Jitter Tx</td>
<td>The average jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Avg Jitter Rx</td>
<td>The average jitter of packets received during an H.323 call, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Max Jitter Tx</td>
<td>The maximum jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.</td>
</tr>
<tr>
<td>Max Jitter Rx</td>
<td>The maximum jitter of packets received during an H.323 call, calculated from sample tests done once per minute.</td>
</tr>
</tbody>
</table>

12 To export the information, click **Download Report** and either **Open** or **Save** the CDR report in Microsoft Excel format for the selected endpoint or in CSV format **For All Selected Endpoints**. Note that only the first 1000 lines of the report are exported to the Excel file.

13 Click **Change Selection** to return to the **Endpoint Usage Report** page to select a different endpoint.
Conference Usage Report

Use the Conference Usage Report option to review usage information about system conferences.

To create a Conference Usage Report:

   An empty Conference Usage Report grid displays.

2. As needed, change the Start: and End: dates to select the date range for the report.
   Select Summary Report or Detail Report. These reports includes the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Name</td>
<td>Name of the conference.</td>
</tr>
<tr>
<td>Conference Scheduler</td>
<td>Name of the user who scheduled the conference.</td>
</tr>
<tr>
<td>Conference Scheduler ID</td>
<td>ID of the user who scheduled the conference.</td>
</tr>
<tr>
<td>Date</td>
<td>Date of the conference.</td>
</tr>
<tr>
<td>Scheduled Start</td>
<td>Scheduled start time of the conference.</td>
</tr>
<tr>
<td>Scheduled Stop</td>
<td>Scheduled stop time of the conference.</td>
</tr>
<tr>
<td>Scheduled Duration</td>
<td>Scheduled duration of the conference.</td>
</tr>
<tr>
<td>Actual Start</td>
<td>The actual time the conference started.</td>
</tr>
<tr>
<td>Actual Stop</td>
<td>The actual time the conference stopped.</td>
</tr>
<tr>
<td>Actual Duration</td>
<td>The actual duration of the conference.</td>
</tr>
<tr>
<td>Total Scheduled Participants</td>
<td>Total number of scheduled participants for the conference.</td>
</tr>
<tr>
<td>Total Actual Participants</td>
<td>Total number of actual participants who attended the conference.</td>
</tr>
</tbody>
</table>

Conference Type Report

Use the Conference Type Report option to review monthly summary information about past RealPresence Resource Manager system conferences.
To create a Conference Type Report

1  Go to Reports > Conference Type Report.

   An empty Conference Type Report grid appears.

2  If areas are enabled and you manage more than one area, you can use the Belongs To Area drop-down list to filter the conference types by area.

3  As needed, change the From: and To: dates to select the date range for the report, and click View.

The Conference Type Report for the selected date range appears. It includes the following information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Information is displayed on a month-by-month basis and an average for the selected months.</td>
</tr>
<tr>
<td>Area</td>
<td>This field is only visible when Areas are enabled. You can only view area-specific information for area(s) that you have permission to manage.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>The number of conferences scheduled with the RealPresence Resource Manager system scheduling interface.</td>
</tr>
<tr>
<td>Ad hoc</td>
<td>The number of conferences that used one or more endpoints that are registered to the RealPresence Resource Manager, but that weren’t scheduled via the RealPresence Resource Manager system scheduling interface. Ad hoc conference information can only be viewed by users with the administrator role. Although users with area administrator roles who manage more than area can view this column, the value will always be zero because ad hoc conferences are not associated with areas. Ad hoc conferences that take place on MCUs that are managed by the Polycom DMA system cannot be monitored by the RealPresence Resource Manager. Monitoring information will be incorrect and inconsistent.</td>
</tr>
<tr>
<td>Multipoint</td>
<td>The number of multipoint conferences scheduled using the RealPresence Resource Manager system scheduling interface.</td>
</tr>
<tr>
<td>Point-to-Point</td>
<td>The number of point-to-point conferences scheduled using one of the RealPresence Resource Manager system scheduling interfaces.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The number of scheduled conferences that used a gateway to reach one or more endpoints.</td>
</tr>
</tbody>
</table>
To create one of the conference type report charts, click the appropriate chart name below the grid. Chart choices include:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Multipoint</td>
<td>The number of scheduled multipoint conferences that used the MCU embedded in a V-Series, VSX-Series, or Polycom HDX-Series endpoint rather than an external MCU such as an RMX MCU.</td>
</tr>
<tr>
<td>Two Person Conferences on MCU</td>
<td>The number of scheduled point-to-point conferences that used an external MCU such as an RMX MCU even through point-to-point conferences do not usually require MCU resources.</td>
</tr>
<tr>
<td>Short</td>
<td>The number of scheduled conferences that were scheduled to last 30 minutes or more, but which actually lasted less than 30 minutes.</td>
</tr>
<tr>
<td>Scheduled Minutes</td>
<td>The sum of the scheduled minutes for all RealPresence Resource Manager system scheduled conferences.</td>
</tr>
<tr>
<td>Executed Minutes</td>
<td>The sum of the actual minutes for all RealPresence Resource Manager system scheduled conferences.</td>
</tr>
<tr>
<td>Total Participants</td>
<td>The sum of the participants that joined RealPresence Resource Manager system scheduled conferences.</td>
</tr>
<tr>
<td>Avg Participants in Multipoint</td>
<td>The average number of participants that joined scheduled RealPresence Resource Manager system multipoint conferences.</td>
</tr>
</tbody>
</table>

To create one of the conference type report charts, click the appropriate chart name below the grid. Chart choices include:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled vs. Ad hoc</td>
<td>A chart that compares the number of scheduled conferences to the number of ad hoc conferences. Ad hoc conference information can only be viewed by users with the administrator role. Although users with area administrator roles who manage more than area can view this column, the value will always be zero because ad hoc conferences are not associated with areas. Ad hoc conferences that take place on MCUs that are managed by the Polycom DMA system cannot be monitored by the RealPresence Resource Manager. Monitoring information will be incorrect and inconsistent.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>A chart that compares the number of point-to-point, multipoint, gateway, and embedded multipoint conferences.</td>
</tr>
<tr>
<td>Scheduled vs. Executed Mins</td>
<td>A chart that compares the number of scheduled minutes to the number executed minutes.</td>
</tr>
</tbody>
</table>
The selected chart dynamically appears below the grid.

5 To export the report:
   a Click Export.
   b In the File Download dialog box, click Save.

### View and Export System Log Files

Many of the RealPresence Resource Manager system components can write a System Log File when they experience an error or issue.

Whether or not they do write a system log file depends upon the system log level. You can change the system log level. See “Change the System Log Level” on page 317.

#### To view System Log Files

1 Go to Reports > System Logs.
   The System Log Files list appears listing the logs for the given time period.

2 To view a log file:
   a Select the log file of interest.
   b Click Open.

3 To export a .zip of all log files:
   a Click Download All.
   b To open the .zip file, in the File Download dialog box, click Open with, and browse to the program you use to open .zip files.
   c To save the .zip file to your local computer, in the File Download dialog box, click Save.
**Change the System Log Level**

**To edit the current system log level**

1. Go to Reports > System Logs.
   
   The System Log Files list appears listing the logs for the given time period. The Current Log Level indicates which log files are being saved.

2. Select the report you want.

3. Click Change Settings.

4. From the Current Log Level menu, select a new value. Choices include:
   
   - Debug
   - Info
   - Warn
   - Error
   - Fatal
   - Off

5. In a redundant configuration, repeat steps 1 and 4 on the redundant server.

**Download Log Files**

You can download a .zip file that includes the log files for the RealPresence Resource Manager system. The log files include the operating system level application, security, and system logs. These logs store events logged by operating system.

**To download the System Logs**

1. Go to Reports > System Log Files.

2. Click Download All.

3. In the File Download dialog box, click Save to save the log file to your local system.

**View and Download Audit Log Files**

You can view and download audit log files.
To view and download audit log files

1. Go to Reports > Audit Log Files.

   The Audit Log Files page appears listing the logs being stored on the system. The following table identifies the RealPresence Resource Manager system audit log files.

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;localhost&gt;_access.log.&lt;timestamp&gt;</td>
<td>Log file that shows every web request that was made from client systems. The system may have more than one such log.</td>
</tr>
<tr>
<td>ResourceManager_audit_jserver.log</td>
<td>Log file that captures security-related authentication issues.</td>
</tr>
<tr>
<td>ResourceManager-firewall.log</td>
<td></td>
</tr>
</tbody>
</table>

2. Select the audit log of interest and click Open.

3. In the File Download dialog box, click Open to view the file or click Save to save the log file to your local system.

Resource Manager System Report

The Resource Manager System Report is not available from the Reports menu, but it can be a useful report. It produces a SystemInfo.txt file that describes the system configuration.

To view Resource Manager System Report

1. Go to Admin > Troubleshooting Utilities.


3. When the File Download dialog box appears, either Open or Save the SystemInfo.txt file:

   The report includes this information.

   Resource Manager VERSION
   Software version : 6.00.00.ER012
   Hardware version : REVISION_B
   LDAP Integration : true

   SECURITY SETTINGS
   System under Secure Mode: false
NETWORK CONFIGURATION
   System name           :  POLYCOM-Dell150
   System IPv4 Address   :  10.47.10.150
   System IPv6 Address   :  N/A
   System IPv6 Link local:  N/A
   System subnet mask    :  255.255.255.0
   System default gateway:  10.47.10.10
   System DNS domain     :  pe.com
   System DNS server 1:  10.47.10.189
   System DNS server 2:  N/A

LICENSE INFO
   Total number of licenses :  100
   Number of licenses in use:  10

CONFERENCE SETTINGS
   Conference Time Warning                   :  true
   Include Conference Owner in new Conference:  false
   Allow Overbooking of dial-In participants :  false
   Conference PIN Length                     :  15

SESSION MANAGEMENT SETTINGS
   Remote Desktop Connection is allowed     :  true
   CMA User Interface timeout (in sec)      :  60
   Max number of sessions per user          :  5
   Max number of sessions per user enabled  :  false
   Max number of sessions per system        :  50
   Max number of sessions per system enabled:  false

LOCAL USER ACCOUNT CONFIGURATION
   Failed login threshold             :  3
   Failed login windows (hours)       :  1
   Lockout duration (minutes)         :  Indefinite
   Account Inactivity threshold (days):  30

LOCAL PASSWORD REQUIREMENTS
   Maximum password age (days)     :  180
   Password warning interval (days):  7
   Number of lowercase letters     :  1
   Number of uppercase letters     :  1
   Minimum length (characters)     :  8
   Minimum password age (days)     :  1
   Number of numbers               :  1
   Reject previous passwords       :  8
   Number of special characters    :  1
   Minimum number of changed characters :  1
   Maximum consecutive repeated characters:  1

CERTIFICATE INFO
Certificate Common Name    :  CMA Self-Signed Certificate
Certificate CRL Version    :  0
Certificate CRL Expired    :  false
Certificate Alias          :
1.2.840.113549.1.9.1=#1613737570706f727440706f6c79636f6d2e636f6d,c
n=cma self-signed
certificate,ou=vsg,o=polycom,l=pleasanton,st=california,c=us
Certificate Issuer         :  Resource Manager Self-Signed
Certificate

REDUNDANCY INFORMATION
   Server 1 IP address:  10.47.10.150
   Server 1 is PRIMARY:  true
   Server 1 is ON      :  true
   Server 2 IP address:  N/A
   Server 2 is PRIMARY:  false
   Server 2 is ON      :  false
   Virtual IP address  :  N/A

DATABASE CONFIGURATION
   Use external DB      :  false
This chapter describes the Polycom® RealPresence® Resource Manager system Dashboard, menu, and actions. It includes these topics:

- “System Dashboard” on page 321
- “Dashboard Buttons” on page 322
- “Dashboard Panes” on page 322
- “System Administration Menu” on page 330

**System Dashboard**

When you log into the RealPresence Resource Manager system with Administrator role and permissions, the system first displays the system Dashboard. Use the system Dashboard to view information about system health and activity levels.

Polycom recommends that you use a minimum monitor display of 1280 x 1024 pixels to view the system Dashboard.

The system Dashboard displays data in an array of charts, forms, data grids, and other graphical displays. It is supremely customizable. You can modify your system Dashboard layout by moving (select the pane title, hold, drag and drop), minimizing, maximizing, closing, and restoring panes. Also note that your changes to the system Dashboard are persistent not just for a session but between logouts and logins.
Dashboard Buttons

In general, the system Dashboard displays information only. However, the following buttons are available from the Dashboard view.

<table>
<thead>
<tr>
<th>Button</th>
<th>Use this button to....</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Panes</td>
<td>Add additional display panes to the system Dashboard. See “Dashboard Panes” on page 322.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the page with current information. To change the frequency of automatic screen refreshes from the default of 5 seconds, click the down arrow and select another option: 15, 30 45, or 60 seconds. The Refresh button flashes when the system refreshes the Dashboard or when you click Refresh.</td>
</tr>
<tr>
<td>Restart ⚡</td>
<td>Shuts down and restarts the system. See “Restart or Shut Down a Polycom RealPresence Resource Manager System” on page 7.</td>
</tr>
<tr>
<td>Shutdown ⚪</td>
<td>Shuts down the system. See “Restart or Shut Down a Polycom RealPresence Resource Manager System” on page 7.</td>
</tr>
</tbody>
</table>

Dashboard Panes

By default the system Dashboard displays the following informational panes:

- “Users Logged In” on page 323
- “Resource Manager Configuration” on page 323
- “Resource Manager Info” on page 324
- “Resource Manager Licenses” on page 325

But you can add or remove panes to customize the system Dashboard. Additional panes that you can add include:

- “Pre-call Status” on page 325
- “Today’s Adhoc Conferences” on page 326
- “Today’s Scheduled Conferences” on page 326
- “Endpoints” on page 327 (multiple, configurable panes)
- “Systems” on page 327
- “Conference Status” on page 328
- “Failed Enterprise Directory Login Attempts” on page 328
- “Redundancy Status” on page 328
- “MCU Status” on page 328 (multiple, configurable panes)
These panes are described in more detail in the following topics.

**Users Logged In**

The Users Logged In pane displays the type and number of users that are currently logged into the system. A sparkline presents the number of logins over time (30 minutes total; updated every 5 minutes so there are 6 data points on the sparkline) for each user type.

The system identifies three user types by their permissions: Administrators, Operators, and Schedulers.

Note that these three user types are not necessarily the same as user roles. For example, users assigned the default Administrator and default Device Administrator roles appear in this pane as Administrators. And users assign the default View Only Scheduler, default Scheduler, and default Advanced Scheduler roles appear in this pane as Schedulers.

For more information, see “Working with Management Roles and Permissions” on page 266.

**Resource Manager Configuration**

The Resource Manager Configuration pane displays information about the configuration of the Resource Manager system, including:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Version</td>
<td>Displays the current version of the software running on the system.</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>Identifies the Dell hardware version of the system.</td>
</tr>
<tr>
<td>CMAD Shipped Version</td>
<td>Displays the version of CMA Desktop for PC that shipped with the version of system software running on the system. Users can download this version of the Polycom CMA software from the Downloads page.</td>
</tr>
<tr>
<td>CMAD Mac Shipped Version</td>
<td>Displays the version of CMA Desktop for MacIntosh that shipped with the version of system software running on the system. Users can download this version of the Polycom CMA Desktop software from the Downloads page.</td>
</tr>
<tr>
<td>Enterprise Directory</td>
<td>Displays the enterprise directory configuration. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—If the system is configured to auto-discover the enterprise directory server.</td>
</tr>
<tr>
<td></td>
<td>• DNA name or IP address of the enterprise directory server—If an enterprise directory server is specified on the system configuration page.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—If the system is not integrated with an enterprise directory server.</td>
</tr>
</tbody>
</table>
### Resource Manager Info

The **Resource Manager Info** pane displays general information about the system, including:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Displays the database source (<strong>Internal</strong> or <strong>External</strong>) and the DNS name or IP address of the database server.</td>
</tr>
<tr>
<td>Time Source</td>
<td>Displays the time server source (<strong>Internal</strong> or <strong>External</strong>) and the IP address of the time server.</td>
</tr>
<tr>
<td>Redundancy</td>
<td>Displays whether or not the system is configured for redundancy. The <strong>Redundancy</strong> field may also show two configuration errors: <strong>Need Virtual IP</strong> or <strong>Secondary Is Down</strong>.</td>
</tr>
<tr>
<td>Remote Alerts</td>
<td>Displays whether or not the system is configured to send remote alert notifications.</td>
</tr>
<tr>
<td>Enterprise Directory DC</td>
<td>If the system is integrated with a domain controller for single sign on authentication, displays the domain name for that domain controller. If the system is not integrated with a single sign on domain controller, this field displays <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Remote Desktop</td>
<td>Displays whether or not Remote Desktop Connection is enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| CPU Utilization        | Displays two views of the system control processor unit (CPU) usage:  
  • A sparkline that presents the CPU usage over time (10 minutes total; updated every 1 minute so there are 10 data points on the sparkline)  
  • A percentage indicator that shows the current usage |
| Paging File            | Displays two views of the system paging file usage:  
  • A sparkline that presents the paging file usage over time (10 minutes total; updated every 1 minute so there are 10 data points on the sparkline)  
  • A percentage indicator that shows the current usage |
| Last JServer Start Time|             |
| Provisioning in Progress| Displays the number of scheduled endpoint provisioning processes that are currently underway. |
| Software Updates in Progress| Displays the number of scheduled endpoint software update processes that are currently underway. |
| Hardware Alarms        | The number of hardware components in the Resource Manager system reporting a warning state. |
Resource Manager Licenses

The Resource Manager Licenses pane displays information about how the system is licensed, including:

- The **Total Number of Licenses** available on the system
- The **Licenses in Use**, which displays two views of the system active calls:
  - A sparkline that presents the license usage over time (60 minutes total; updated every 5 minutes so there are 12 data points on the sparkline).
  - A percentage indicator that shows the current usage.

Pre-call Status

The Pre-call Status pane displays information about the next conference or conferences that are scheduled to launch including:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to Conference</td>
<td>Displays the system-defined pre-call status reporting time of 10 minutes. In other words, the Pre-call Status pane always reports on conferences that are scheduled to start in the next 10 minutes.</td>
</tr>
<tr>
<td>Scheduled to Launch</td>
<td>Displays the number of conferences scheduled to start in the next 10 minutes.</td>
</tr>
</tbody>
</table>
Today’s Adhoc Conferences

The Today’s Adhoc Conferences pane displays information about the ad hoc conferences started by video endpoints registered to the Resource Manager system. For the current day (starting at 0:00 and ending at 24:00), it displays:

- The number of ad hoc conferences that were Completed for the current day
- The number of ad hoc conferences that are Active at the current time
- A bar chart that displays the number of ad hoc conferences (vertical axis) plotted against time of day (horizontal axis)

Note

Ad hoc conferences that take place on MCUs that are managed by the Polycom DMA system cannot be monitored by the RealPresence Resource Manager. Monitoring information will be incorrect and inconsistent.

Today’s Scheduled Conferences

The Today’s Scheduled Conferences pane displays information about the scheduled conferences managed by the Resource Manager system. For the current day (starting at 0:00 and ending at 24:00), it displays:

- The number of scheduled conferences that were Completed that day
- The number of scheduled conferences that are Active at the current time
- The number of scheduled conferences that are yet to occur (Future)
- A bar chart that displays time on the linear axis plotted against the number of scheduled conferences on the horizontal axis
Endpoints

The system allows you to add multiple **Endpoints** panes so you can create your own scheme for grouping and monitoring endpoints. When you add an **Endpoints** pane, you can give the pane a meaningful name and select which endpoints to monitor. You can save the pane, create others as needed. You can also reconfigure an **Endpoints** pane using the configuration tool.

**Endpoints** panes display the following information:

- The number of endpoints being monitored
- The number of monitored endpoints that are **In a Call**
- The number of monitored endpoints that are **Online**
- The number of monitored endpoints that are **Offline**

In addition, the **Endpoints** pane identifies any monitored endpoints that are experiencing alert conditions. If you click on an endpoint in the list, the system displays the **Endpoint > Monitor View**.

Finally, click **View Endpoint** to see the **Status, Name, Alias, IP Address, Owner, and Site** for the monitored endpoints. This status information is sent by the endpoints to the Resource Manager system.

Systems

The **Systems** pane displays summary information about the devices registered with the Resource Manager system, including:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints</td>
<td>The number of endpoints registered with the Resource Manager system.</td>
</tr>
<tr>
<td>VVXs</td>
<td>The number of VVX systems registered with the Resource Manager system.</td>
</tr>
<tr>
<td>MCUs</td>
<td>The number of MCUs registered with the Resource Manager system.</td>
</tr>
<tr>
<td>Gatekeepers</td>
<td>The number of gatekeepers identified to the Resource Manager system.</td>
</tr>
<tr>
<td>Gateways</td>
<td>The number of individual H.323 cards and/or IP blades in Polycom MCUs are assigned the device type of GW/MCU during registration.</td>
</tr>
<tr>
<td>Rooms</td>
<td>The number of rooms defined with the Resource Manager system.</td>
</tr>
<tr>
<td>SBCs</td>
<td>The number of Acme SBCs defined with the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>VBPs</td>
<td>The number of Polycom VBPs defined with the Resource Manager system.</td>
</tr>
</tbody>
</table>
If any of the devices registered with the Resource Manager system experience a fault, the Systems pane also displays an alert icon. Click the alert icon to see the Endpoint or Network Device view and get more information about the alert.

### Conference Status

The Conference Status pane displays the list of active conferences. (see screenshot) plus 2 of 6 participants online.

Click on conference title to go to conference monitor view for that conference.

### Failed Enterprise Directory Login Attempts

The Failed AD Login Attempts pane displays:

- The total number of Failed Logins for Active Directory users in the last 24 hour period.
- The domain\username for the Active Directory users whose login attempts failed and how many times they failed. Click the domain\username to view the date and time for the failed attempts.

### Redundancy Status

The Redundancy Status pane displays information about the Resource Manager system redundancy configuration, including:

- Whether or not the system is configured for redundancy. Possible values for Status are Configured or Not Configured.
- The Virtual IP Address for the redundant system. If it is not configured for redundancy, the value will be No.
- The IP address of the Active Server
- The IP address of the Backup Server

### MCU Status

The system allows you to add multiple MCU Status panes so you can create a pane for all or individual MCUs registered with the Resource Manager system. When you add an MCU Status pane, you can give the pane a meaningful name and either select an MCU to monitor or select All MCUs. You can save the pane, create others as needed. You can also reconfigure an MCU Status pane using the configuration tool.

The MCU Status pane for All MCUs displays the following information:
The **MCU Status** pane for **All MCUs** also lists all of the registered MCUs and displays the Errors and Warnings for the MCUs.

The **MCU Status** pane for an individual MCU displays the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>Displays the cumulative number of alarms on the MCU.</td>
</tr>
<tr>
<td>Warnings</td>
<td>Displays the cumulative number of warnings for all of the registered MCUs.</td>
</tr>
<tr>
<td>Active Conferences</td>
<td>Displays the number of active conferences currently being hosted by the MCU.</td>
</tr>
<tr>
<td>Number of Audio Ports</td>
<td>Displays the number of dedicated audio ports configured on the MCU.</td>
</tr>
</tbody>
</table>
| Audio Ports Utilization | Displays two views of the MCU audio port usage:  
• A sparkline that presents the audio port usage over time  
• A percentage indicator that shows the current usage |
| Number of Video Ports | Displays the number of video ports configured on the MCU. |
| Video Ports Utilization | Displays two views of the MCU video port usage:  
• A sparkline that presents the video port usage over time  
• A percentage indicator that shows the current usage |
| Expected Port Utilization | A timeline that shows how many ports are scheduled for conferences within the next 45 minutes. |

This status information is sent by the MCU to the Resource Manager system.

---

**Note**

If your system has areas enabled, you will only be able to view MCUs that belong to areas that you have been assigned to manage.
In addition, the **MCU Status** pane identifies when the monitored MCU is experiencing alert conditions.

**System Administration Menu**

The system **Admin** menu gives users with administrative permissions access to the day-to-day management tasks they need to monitor, maintain, and troubleshoot the Resource Manager system. Besides the **Dashboard**, it lists these selections:

<table>
<thead>
<tr>
<th>Selection</th>
<th>Use this selection to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Conference Templates</td>
<td>Manage (add, edit, and delete) direct conference templates. See “Direct Conference Templates” on page 334.</td>
</tr>
<tr>
<td>Conference Settings</td>
<td>Enable or disable Conference Auto-launch and Conference Time Warning. See “Conference Settings” on page 347.</td>
</tr>
<tr>
<td>Provisioning Profiles</td>
<td>Manage (add, edit, and delete) automatic or scheduled provisioning profiles.</td>
</tr>
<tr>
<td>Software Updates</td>
<td>Manage (add, edit, and delete) automatic or scheduled software update packages.</td>
</tr>
<tr>
<td>Rooms</td>
<td>Manage (add, edit, and delete) rooms in the Resource Manager system directory.</td>
</tr>
<tr>
<td>Areas</td>
<td>Manage Areas for a Resource Manager system.</td>
</tr>
<tr>
<td>Directories</td>
<td>Manage the directories available to the Resource Manager system including the enterprise directory, address books, or Global Address Book.</td>
</tr>
<tr>
<td>Server Settings</td>
<td>Configure the basic Resource Manager system, which includes the network, system time, database, directory, licensing, redundancy, branding, GAB, remote alert, and E-mail set up.</td>
</tr>
<tr>
<td>SNMP Settings</td>
<td>Manage SNMP messaging for the Resource Manager system.</td>
</tr>
<tr>
<td>Management and Security</td>
<td>Upgrade the Resource Manager system and configure the certificate, security, and endpoint management set up.</td>
</tr>
<tr>
<td>Topology</td>
<td>Edit the default Resource Manager system <strong>Site Topology</strong> settings (which includes the definition of sites, site links, network clouds, and territories) to support your network topology and video call routing.</td>
</tr>
<tr>
<td>Alert Settings</td>
<td>Configure the Resource Manager system to send E-mail alerts for specified system or endpoint events.</td>
</tr>
<tr>
<td>Selection</td>
<td>Use this selection to...</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Backup System Settings</td>
<td>Download a .zip archive file containing all configuration information necessary to restore the system.</td>
</tr>
<tr>
<td>Uploads</td>
<td>Upload SIP URI data to the Resource Manager system.</td>
</tr>
<tr>
<td>Troubleshooting Utilities</td>
<td>Access all of the troubleshooting information and utilities the Resource Manager system has available.</td>
</tr>
<tr>
<td>Report Administration</td>
<td>Configure report administration settings including retention periods, etc.</td>
</tr>
</tbody>
</table>
Understanding Conference Templates and Settings

This chapter describes information about conference templates and settings within the Polycom® RealPresence® Resource Manager system. This chapter includes the following sections:

- “Direct Conferences vs. Pooled Conferences” on page 333
- “Direct Conference Templates” on page 334, define most of the settings that become the defaults for a direct conference.
- “DMA (Pooled) Conference Templates” on page 345
- “Conference Settings” on page 347, are global system-wide settings that apply to all scheduled conferences.

Direct Conferences vs. Pooled Conferences

The RealPresence Resource Manager system allows you to use two types of Future (scheduled) conferences: direct conferences and pooled conferences.

- **Direct Conferences** end on RMX devices managed by the RealPresence Resource Manager system. Users with the administrator role can create direct conference templates that can be used for direct conferences. The direct conference template can be defined with the RealPresence Resource Manager system or explicitly identify an existing RMX profile which identifies the settings the RMX should use to control the conference.

- **Pooled Conferences** end on resources managed by the Polycom DMA system (pool orders). Conference templates for pooled conferences are created and maintained on the DMA system.
Direct Conference Templates

You can create direct conference templates to be used for Direct Conferences. Direct Conference templates allow you to create various combinations of settings to apply to scheduled conferences.

Conference templates for Pooled Conferences are created and managed on the Polycom DMA system.

Users assigned the Administrator role can add or edit Direct Conference Templates. They can also identify (by user role) which users have access to which Direct Conference Templates. Then users select from the different templates available to them to switch between different combinations of conference settings.

If using an existing profile on the RMX system, the RealPresence Resource Manager system administrator must manually synchronize the settings in the RealPresence Resource Manager system conference template and its associated RMX profile.

Alternatively, you can configure the RMX profile settings in the RealPresence Resource Manager system conference template, which is used by all RMX systems in the conference. For more information about the RMX profile settings, see the Polycom® RMX® 1500/2000/4000 Administrator’s Guide.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique and meaningful name for the template, which can be up to 32 characters long.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a meaningful description (ASCII only) of the conference settings template.</td>
</tr>
<tr>
<td>Audio-Only Template</td>
<td>Select this option to designate the template as an audio-only template. Selecting this option disables many settings.</td>
</tr>
<tr>
<td>Supported MCUs</td>
<td>Specify the supported MCU type. Possible values include: RMX</td>
</tr>
<tr>
<td>Always Use MCU</td>
<td>When selected, an MCU is used for the scheduled conference, regardless of the number of participants. When not selected, an MCU is used only when necessary.</td>
</tr>
</tbody>
</table>
### Dial Options
These settings apply only to video conferences. The video dial options are:
- **Dial-In Only** (all participants dial into the conference)
- **Dial-Out Only** (all participants are called by the system)
- **Dial-In + Dial-Out** (The person setting up the conference can specify which participants must dial into the conference and which participants are called by the system.)

### Assign Area
Select an area to which to assign this template. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.

### Template will be available to users with the selected roles...
Select the roles to which users must be assigned for them to see this template when scheduling conferences.

### Available Roles
The list of roles defined to the RealPresence Resource Manager system.

### Selected Roles
The list of roles that can use the conference template being defined.

### Common Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meet Me Per Conference</strong></td>
<td>When selected, only one dial-in number is assigned to the conference. When cleared, each dial-in participant is assigned a different dial-in number.</td>
</tr>
</tbody>
</table>
| **Video Mode**               | Sets the video layout for the conference. The default is **Video Switching Mode**. To change to a **Continuous Presence** layout or mode, click the switching icon and select a layout option. The video mode determines the initial layout on an endpoint's display during a multipoint conference. This option requires an MCU. This option is not available for RMX systems if you select any of the following:  
  - **Auto layout** option (**RMX Video Settings**)  
  - **Video switching** option (**RMX General Settings**)  
  - **Telepresence mode** is On (**RMX Video Settings**)  
  **Note** Make sure you have defined video endpoint systems and boards so that they are available for selection in continuous presence layouts. |
### Presentation Mode

- Select to enable **Presentation Mode**. In this mode, the system uses the selected layout to display all participants. When a participant’s speech exceeds a predefined time (30 seconds), the system identifies the participant as the lecturer and changes to **Lecture Mode**. The video mode for the other participant’s automatically changes to full screen, displaying the lecturer, while the lecturer’s endpoint displays participants in the video mode defined previously. When another participant starts talking, the system changes back to **Presentation Mode** and the conference returns to its predefined video layout.

- Clear this option to disable **Presentation Mode**. All participants see the conference in the video mode defined elsewhere.

This option is not available if you select any of the following:
- **Video switching** option (RMX General Settings)
- **Same layout** option (RMX Video Settings)
- **Telepresence mode** is **On** (RMX Video Settings)

**Note**
- RMX 1000 systems do not support **Lecture Mode**, **Presentation Mode**, or **Lecture View Switching**.

### Speed (Kbps)

Sets the speed for the conference, which applies to both point-to-point and multipoint calls.

**Note**
If you use an RMX system profile for conferences that land on an RMX system, the speed designated here is used to reserve bandwidth and must match the line rate defined in the RMX system profile that is identified in the **Profile Name** field.

### Lecturer View Switching

Select this option to enable automatic switching of participants on the Lecturer’s screen when **Lecture Mode** is set to **Presentation Mode** and the number of participants exceeds the number of windows identified by the video mode defined elsewhere.

This option is not available if you select any of the following:
- **Same layout** option (RMX Video Settings)
- **Telepresence mode** is **On** (RMX Video Settings)

**Note**
RMX 1000 systems do not support **Lecture Mode**, **Presentation Mode**, or **Lecture View Switching**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation Mode</td>
<td>Select to enable <strong>Presentation Mode</strong>. In this mode, the system uses the selected layout to display all participants. When a participant's speech exceeds a predefined time (30 seconds), the system identifies the participant as the lecturer and changes to <strong>Lecture Mode</strong>. The video mode for the other participant’s automatically changes to full screen, displaying the lecturer, while the lecturer’s endpoint displays participants in the video mode defined previously. When another participant starts talking, the system changes back to <strong>Presentation Mode</strong> and the conference returns to its predefined video layout. Clear this option to disable <strong>Presentation Mode</strong>. All participants see the conference in the video mode defined elsewhere. This option is not available if you select any of the following: <strong>Video switching</strong> option (RMX General Settings) <strong>Same layout</strong> option (RMX Video Settings) <strong>Telepresence mode</strong> is <strong>On</strong> (RMX Video Settings). <strong>Note</strong> RMX 1000 systems do not support <strong>Lecture Mode</strong>, <strong>Presentation Mode</strong>, or <strong>Lecture View Switching</strong>.</td>
</tr>
<tr>
<td>Speed (Kbps)</td>
<td>Sets the speed for the conference, which applies to both point-to-point and multipoint calls. <strong>Note</strong> If you use an RMX system profile for conferences that land on an RMX system, the speed designated here is used to reserve bandwidth and must match the line rate defined in the RMX system profile that is identified in the <strong>Profile Name</strong> field.</td>
</tr>
<tr>
<td>Lecturer View Switching</td>
<td>Select this option to enable automatic switching of participants on the Lecturer’s screen when <strong>Lecture Mode</strong> is set to <strong>Presentation Mode</strong> and the number of participants exceeds the number of windows identified by the video mode defined elsewhere. This option is not available if you select any of the following: <strong>Same layout</strong> option (RMX Video Settings) <strong>Telepresence mode</strong> is <strong>On</strong> (RMX Video Settings) <strong>Note</strong> RMX 1000 systems do not support <strong>Lecture Mode</strong>, <strong>Presentation Mode</strong>, or <strong>Lecture View Switching</strong>.</td>
</tr>
</tbody>
</table>
Understanding Conference Templates and Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use existing profile   | Select to use an existing RMX system profile. Clear to set all of the RMX system profile settings here in the conference template. This method ensures that the RMX profile settings are the way you want them and avoids maintaining identical profiles on all RMX systems.  
  **Note**  
  With this option selected, conferences fail if they land on an RMX system and a valid RMX system profile is not specified below. |
| RMX profile name       | Identifies the RMX system profile for the conference, if the conference is hosted on an RMX system. Enter the RMX system profile routing name, which is generally (but not always) the same as the profile name as specified in the RMX system. |

### RMX General Settings > Conference Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Video switching (VSW)  | In Video Switching mode, all participants see the same video picture (full screen). The current speaker is displayed in full screen on all the participants’ endpoints, while the speaker sees the previous speaker. Switching between participants is voice-activated; whenever a participant starts to speak, he or she becomes the conference speaker and is viewed on all screens.  
  When selected, the conference is of ultra-high quality video resolution, in a special conferencing mode which implies that all participants must connect at the same line rate and use HD video.  
  This feature utilizes the resources more wisely and efficiently by:  
  • Saving utilization of video ports (1 port per participant as opposed to 4 ports in CP mode).  
  • Video display is in full screen mode only.  
  Drawbacks of this feature are that all participants must connect at the same line rate, (for example, HD), and all participants with endpoints not supporting HD will connect as secondary (audio only).  
  Video layout changes are not enabled during a conference.  
  If HD 1080p is selected, endpoints that do not support HD 1080p resolution are connected as secondary (audio only) participants.  
  **Note**  
  Video Switching conferencing mode is unavailable to ISDN participants. |
## Resolution
Possible values include:
- H.264 SD 30(v7 with MPM+ or MPMx)
- H.264 720p60(v7 with MPM+ or MPMx)
- H.264 720p30
- H.264 1080p30(MPM+ or MPMx)

## RMX General Settings > Advanced Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto redialing | Instructs the RMX system to automatically redial IP and SIP participants that have been abnormally disconnected from the conference.  
- The RMX system will not redial an endpoint that has been disconnected from the conference by the participant.  
- The RMX system will not redial an endpoint that has been disconnected or deleted from the conference by an operator or administrator. |
| Encryption     | Activate encryption for the conference                                         |
| LPR            | Activate lost packet recovery (LPR) for the conference.                      |
|                | **Note** LPR can be enabled for VSW conferences, but H.320 and SIP participants will not be able to connect. |
| Auto terminate | When selected (default), the conference automatically ends when the termination conditions are met:  
- **Before first joins** — No participant has connected to a conference during the n minutes after it started. Default idle time is 10 minutes.  
- **At the end - After last participant quits** — All the participants have disconnected from the conference and the conference is idle (empty) for the predefined time period. Default idle time is 1 minute.  
- **At the end - When last participant remains** — Only one participant is still connected to the conference for the predefined time period (excluding the recording link which is not considered a participant when this option is selected). This option should be selected when defining a profile that will be used for Gateway Calls and you want to ensure that the call is automatically terminated when only one participant is connected. Default idle time is 1 minute. |
Understanding Conference Templates and Settings

**RMX Video Quality > People Video Definition**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Video quality | Optimizes the video quality based on the amount of movement contained in the conference video. Possible values include:  
  • **Motion**—Provides a higher frame rate without increased resolution.  
  • **Sharpness**—Provides a higher video resolution and requires more system resources. |

| Max resolution (v7) | Depending on whether MPM+ or MPMx cards are installed, the possible values include:  
  • **Auto**  
  • **CIF**  
  • **HD 1080**  
  • **HD 720**  
  • **SD** |

| Video clarity (MPM+ and MPMx only) | Applies video enhancing algorithms to incoming video streams of resolutions up to and including SD. Clearer images with sharper edges and higher contrast are sent back to all endpoints at the highest possible resolution supported by each endpoint.  
This option is not available if you select any of the following:  
  • **Motion** option for **Video quality**  
  • **Video switching (VSW)** option (RMX General Settings) |

| Auto brightness (v7) | Detects and automatically adjusts the brightness of video windows that are dimmer than other video windows in the conference layout.  
This option is not available if you set **Telepresence mode** to **On** (RMX Video Settings). |

**RMX Video Quality > Content Video Definition**

| Content settings | Select the transmission mode for the content channel:  
  • **Graphics** — Basic mode, intended for normal graphics.  
  • **Hi-resolution graphics** — Higher bit rate intended for high resolution graphic display.  
  • **Live video** — Content channel displays live video. Selection of a higher bit rate for the content results in a lower bit rate for the people channel. |
## Content protocol

The possible values are:
- **H.263** – Content is shared using H.263 even if some endpoints have H.264 capability.
- **Up to H.264** – H.264 is the default content sharing algorithm. When selected:
  - Content is shared using H.264 if all endpoints have H.264 capability.
  - Content is shared using H.263 if all endpoints do not have H.264 capability.
  - Endpoints that do not have at least H.263 capability can connect to the conference but cannot share content.

## RMX Video Settings

### Send content to legacy endpoints (MPM+ and MPMx only)

Content can be sent to H.323/ SIP/ISDN endpoints that do not support H.239 content (legacy endpoints) over the video (people) channel.

This option is not available if you select any of any of the following:
- **Video switching (VSW) option** (RMX General Settings)
- **Same layout** option

**Note**

When enabled, additional video resources are allocated to the conference.

### Same layout

Select this option to force the selected layout on all participants in a conference. Displays the same video stream to all participants and personal selection of the video layout is disabled. If participants are forced to a video layout window, they can see themselves.

This option is not available if you select any of the following:
- **Video switching (VSW) option** (RMX General Settings)
- **Telepresence mode is On** (RMX Video Settings)

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Content protocol | The possible values are:  
  - **H.263** – Content is shared using H.263 even if some endpoints have H.264 capability.  
  - **Up to H.264** – H.264 is the default content sharing algorithm. When selected:  
    - Content is shared using H.264 if all endpoints have H.264 capability.  
    - Content is shared using H.263 if all endpoints do not have H.264 capability.  
    - Endpoints that do not have at least H.263 capability can connect to the conference but cannot share content. |
| RMX Video Settings |  
  **Send content to legacy endpoints (MPM+ and MPMx only)**  
  Content can be sent to H.323/ SIP/ISDN endpoints that do not support H.239 content (legacy endpoints) over the video (people) channel.  
  This option is not available if you select any of any of the following:  
  - **Video switching (VSW) option** (RMX General Settings)  
  - **Same layout** option  
  **Note**  
  When enabled, additional video resources are allocated to the conference. |
| Same layout | Select this option to force the selected layout on all participants in a conference. Displays the same video stream to all participants and personal selection of the video layout is disabled. If participants are forced to a video layout window, they can see themselves.  
  This option is not available if you select any of the following:  
  - **Video switching (VSW) option** (RMX General Settings)  
  - **Telepresence mode is On** (RMX Video Settings) |
Understanding Conference Templates and Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto layout                   | Select this option to have the system automatically select the conference layout based on the number of participants currently connected to the conference. When a new video participant connects or disconnects, the conference layout automatically changes to reflect the new number of video participants. Clear this option to manually select a layout for the conference using the Video Mode options. This option is not available if you select any of any of the following:  
  • Video switching (VSW) option (RMX General Settings)  
  • Lecture View Switching option (Common Settings)  
  • Telepresence mode is On (RMX Video Settings) |

| Telepresence mode (v6)        | The possible values are:  
  • **Auto** (Default) - If any ITP (Immersive Telepresence) endpoints are detected, ITP features are applied to the conference video for all participants. The ITP features are dynamic. If all ITP endpoints disconnect from the conference, normal conference video resumes for all participants. ITP features resume for all participants if an ITP endpoint reconnects to the conference.  
  • **On** - ITP features are applied to the conference video for all participants regardless of whether there are ITP endpoints connected.  
  • **Off** - Normal conference video. |

**Note**  
This field is enabled only if the RMX system is licensed for Telepresence Mode.

| Telepresence layout mode (v6) | Enables VNOC operators and Polycom Multi Layout Applications to retrieve Telepresence Layout Mode information from the RMX.  
The possible values include:  
  • **Manual**  
  • **Continuous Presence** - Room continuous presence (default)  
  • **Room Switch** - Voice activated room switching |

| RMX Audio Settings            | (Supported only with MPM+ or MPMx cards.) Enables an algorithm to search for and detect sounds outside the normal range of human speech (such as echo) and automatically mute them when detected. |

---

Polycom, Inc.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyboard noise suppression</td>
<td>(Supported only with MPM+ or MPMx cards.) Enables an algorithm to search for and detect keyboard noises and automatically mute them when detected.</td>
</tr>
<tr>
<td>Audio clarity (v7)</td>
<td>(Supported only with MPM+ or MPMx cards.) Improves received audio from participants connected via low audio bandwidth connections, by stretching the fidelity of the narrowband telephone connection to improve call clarity. The enhancement is applied to the following low bandwidth (8kHz) audio algorithms: G.729a and G.711.</td>
</tr>
</tbody>
</table>
| RMX Skins                     | Select the skin you want. Skins modify the background and frames. With the top two skin options, the frames fill the screen with their borders touching. These options are not available if you select any of the following:  
- Video switching (VSW) option (RMX General Settings)  
- Telepresence mode is On (RMX Video Settings) |
| RMX Conference IVR            |                                                                       |
| Override default conference IVR service | Select to override the default conference Interactive Voice Response (IVR).                                                                 |
| Conference IVR service       | If you selected the override option above, enter the name of the conference IVR service you want to use. All RMX systems that could be used must have the same conference IVR service set up. |
Conference requires chairperson

Select this option to require that a video chairperson control the conference from his or her video endpoint system. When this option is implemented, the system will assign a 15-digit password that the conference chairperson must enter to control the conference. The conference scheduler can change this system-assigned password to any 15-digit number.

In this case:
- The video chairperson must have a video endpoint system.
- The conference requires an MCU.
- All conference participants remain in the waiting room and cannot join the conference until the conference chairperson enters the conference.

H.243 chair control allows an endpoint to control the conference using the H.243 chair control feature. The chairperson can disconnect participants, force the use of a continuous presence video layout, and terminate the conference.

**Notes**

- Set in the RMX system profile for RMX 2000/4000 systems
- The RMX 1000 system does not support the Chairperson feature.

### RMX Recording

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable recording</td>
<td>Enables the recording settings. If no Recording links are found, an error message is displayed.</td>
</tr>
<tr>
<td>Record conference</td>
<td>The possible values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Immediately</strong> – Conference recording is automatically started upon connection of the first participant.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Upon request</strong> – The operator or chairperson must initiate the recording (manual).</td>
</tr>
<tr>
<td>Recording link (v7)</td>
<td>Enter the name of the Recording link you want to use. The recording link defines the connection between the conference and the recording system to be used for conference recording. All RMX systems that could be used must have the same recording link set up.</td>
</tr>
<tr>
<td>Audio only</td>
<td>Records only the audio channel of the conference.</td>
</tr>
<tr>
<td>Indication of recording</td>
<td>Displays a recording icon to all conference participants informing them that the conference is being recorded. The recording icon is replaced by a paused icon when conference recording is paused.</td>
</tr>
</tbody>
</table>
Direct Conference Template Considerations for Multi-Tenancy

- When areas are enabled, the templates available for a given conference depend on the area to which the conference owner belongs. Only templates belonging to the same area as the conference owner are available to use when scheduling a conference.

- When areas are enabled, be sure to give your area-specific names to your templates. This is particularly helpful if you have schedulers who have been given permission to manage more than one area.

Direct Conference Template Best Practices

The RealPresence Resource Manager system has a Default Template. Administrators with Conference Setup permissions can edit the Default Template and create additional templates with different settings.

When scheduling a conference, the Default Template, which is available to all users, is selected by default. Schedulers can select a different conference template from the list of templates an administrator has made available to them. Users with advanced scheduling permissions can edit the template settings for a specific scheduled conference. These changes apply only to the specified conference.

Use these best practices when working with conference templates.

- For the Default Template, select settings that are the lowest common values for all device types. This ensures that all conferences scheduled with the Default Template can successfully launch on whatever devices the system has available at the time.

- The template names Default Template and Default Audio Templates are stored in the system database and their names are not localized into other languages. If you wish to localize their names into your language, edit the templates and enter new names for them.

- When creating new templates, give them meaningful purposes and names so that your users can easily identify the differences between template choices. For example, identify templates according to maximum bit rate, specific features implemented by the template (for example, Lecture Mode or Chairperson Control).

Multi-Tenancy Consideration

If your RealPresence Resource Manager system has areas enabled, be sure to give your area-specific names to your templates. This is particularly helpful if you have schedulers who have been given permission to manage more than one area.
• Remember that using an existing RMX system profile will override settings specified when scheduling a conference through the Polycom Resource Manager system. To ensure consistent and expected behavior, make sure to synchronize and lock down RMX profiles and Polycom Resource Manager system conference templates.

The RealPresence Resource Manager systems does not support scheduling direct conferences on third-party MCUs. Template settings apply only to the RMX devices.

DMA (Pooled) Conference Templates

Both Pooled Conferences and Anytime Conferences are enabled when your RealPresence Resource Manager system is integrated with a Polycom DMA system. These conference types use conference templates that are created and managed in the Polycom DMA system.

This section includes the following topics:
• “DMA System Conference Templates for Multi-Tenancy” on page 345
• “Establish Naming Conventions for DMA System Templates” on page 345
• “Considerations for Anytime Conference Templates” on page 346

DMA System Conference Templates for Multi-Tenancy

DMA system conference templates cannot be assigned to a specific area. Area schedulers will be able to select from a list of all DMA system templates, regardless of the area to which they manage. You should implement a template naming convention to indicate to an area scheduler which DMA templates apply to his purview; for example, areal_template.

Establish Naming Conventions for DMA System Templates

By default, all DMA system conference templates are made available to conference schedulers who have permission to create pooled conferences and anytime conferences. To differentiate which DMA system conference templates should be used for which conferences, you should implement a naming convention that informs the scheduler which conference template is appropriate.
**Anytime Conference Templates**

For example, you could prefix a template designed for use with anytime conferences with the word “anytime”; for example, `anytimeconf_standard`, `anytimeconf_autoterminate`, `anytimeconf_nochair`, and so on.

**Considerations for Anytime Conference Templates**

An anytime conference is initiated when the first person calls into the conference and triggers the hosting bridge to dial-out to the remaining conference participants.

Once an Anytime conference is configured, conferences can be started at any time by authorized participants. The following events occur when a new Anytime conference is added:

- A participant with scheduling permissions creates a new Anytime conference and the conference is assigned a virtual meeting room (VMR) number.

- An **Chairperson passcode** is automatically generated and may be required to launch an Anytime conference (depending on your conference template). The owner receives the owner passcode needed to launch the conference via the meeting e-mail.

- Depending on the conference template settings, all dial-out participants are automatically called either when first participant dials the VMR number or the conference owner dials the VMR and enters the owner passcode.

- If the conference template requires a chairperson, dial-in participants are placed on hold until someone dials in and enters the chairperson passcode.

- The conference continues until all participants hang up the call, unless your template includes an auto-terminate setting.

**Configure Auto-Terminate**

Anytime conferences do not have designated start and end times. As a result, the conference may be left open and the VMR in use if the last caller does not hang up. You can mitigate this occurrence by configuring the DMA conference template to use an RMX profile that has Auto-Terminate enabled.

For more information about RMX profiles and how to use an existing RMX profile for a DMA conference template, see *Polycom DMA 7000 System Operations Guide*. 
Initiate Conference Dial-out

You can configure the DMA system conference template to define who can trigger the dial-out to participants. You use the Conference requires chairperson setting to determine when dial-outs are initiated. Remember to use an intuitive naming convention for DMA system conference templates.

- When you enable the Conference requires chairperson setting, the dial-out process will begin when the chairperson dials into the conference. An example name for a template with this setting could be Anytime Conference - Chair Starts Dial-Outs.

- If you leave this check box unmarked, the dial-out process will begin when the first person dials into the conference. No chairperson passcode is needed. An example name for a template with this setting could be Anytime Conference - 1st Dial-in Starts Dial-Outs.

Conference Settings

Conference settings apply to conferences scheduled using the RealPresence Resource Manager system. These settings include:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Time Warning</td>
<td>Specifies whether or not the Polycom Resource Manager system sends a message to video endpoints in a conference to warn the endpoint users that their conference is scheduled to end. The system sends the message 15 minutes and 5 minutes before the conference is scheduled to end. To support this feature, the video endpoint system must be capable of receiving a system Send Message action. By default, Conference Time Warning is enabled.</td>
</tr>
<tr>
<td>Automatically Include Conference Owner (Scheduler) in New Conferences</td>
<td>Select this option when you wish the system to always include the person scheduling the conference as a conference participant. Do not select this option if your organization has assistants or operators schedule conferences for others.</td>
</tr>
</tbody>
</table>

Note

This feature is not related to the MCU-based End Time Alert Tone feature.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow overbooking of dial-in participants</td>
<td>Select this option to allow schedulers to schedule dial-in participants to dial into multiple conferences, but the system reserves resources for the participant for only the first scheduled conference</td>
</tr>
<tr>
<td>Conference and chairperson passcode length</td>
<td>Designate the required length of the system-generated conference and chairperson passcodes. The acceptable length for both of these passcodes is 9 to 16 characters. By default, the required length for both of these passcodes is set to 15 characters.</td>
</tr>
</tbody>
</table>

**Note**

- Depending on the system settings, the scheduler may be allowed to change the conference or chairperson passcode. However, the passcode length requirement still applies.
- If an administrator changes the passcode length here at the same time a scheduler edits the passcode settings for a scheduled conference, the scheduling operation may use either the old or the new length, depending on the exact timing.
View the Direct Conference Templates List

To view the Direct Conference Template list

- Go to Admin > Direct Conference Templates.

The Direct Conference Templates list appears.
Add a Direct Conference Template

To add a direct conference template

1. Go to Admin > Direct Conference Templates.
2. On the Direct Conference Templates list, click Add.
3. Complete the General Info and MCU Settings sections of the Add Conference Template dialog box first. Your selection for MCU Settings affect your choices in the Video Settings section. For more information on the Add Conference Template dialog box, see “Direct Conference Templates” on page 334.
4. Complete the Video Settings and Conf Settings sections of the Add Conference Template dialog box.
5. Click OK.

The new template appears in the Direct Conference Template list.

The RealPresence Resource Manager system does not validate the Conference Template settings. When you create a new conference template, you must make certain that the settings match the capabilities of the MCUs or endpoints.

Edit a Direct Conference Template

To edit a conference template

1. Go to Admin > Direct Conference Templates.
2. On the Direct Conference Templates list, select the template of interest and click Edit.
3. Edit the General Info, Video Settings, MCU Settings, and Conf Settings sections of the Edit Conference Template dialog box as required.

If you change the conference template Speed setting and there are scheduled conferences using that template, all endpoints in the scheduled conferences are reset to whichever is less: the new template Speed or the maximum speed that the endpoint supports.

4. Click OK.
Delete a Direct Conference Template

To delete a conference template
1 Go to Admin > Direct Conference Templates.
2 On the Direct Conference Templates list, select the template of interest and click Delete.
3 Click Yes to confirm the deletion.

Set Conference Settings

To specify conference settings
1 Go to Admin > Conference Settings.
2 On the Conference Settings page, make the required selections. “Conference Settings” on page 347.
3 Click Update.

Disable Conference Auto-Launch

To disable conference auto-launch
1 Go to Admin > Conference Settings.
2 In the Conference Auto-Launch section of the Conference Settings page, check the Disabled check box.
3 Click Update.

Disable Conference Time Warning

To disable the conference time warning
1 Go to Admin > Conference Settings.
2 In the Conference Time Warning section of the Conference Settings page, clear the Enabled check box.
3 Click Update.
Overbooking Dial-in Participants

A user with the administrator role can configure the system to allow scheduler’s to overbook dial-in participants. In this case, dial-in participants can be scheduled to dial into multiple conferences, but the system reserves resources for the participant for only the first scheduled conference. Dial-out participants cannot be scheduled into multiple conferences.

Schedulers can only overbook dial-in participants if they select a conference template that has the Video Dial Option set to Dial-In Only. A conference template that has the Video Dial Option set to Dial In+Dial Out will not work for this purpose.

To allow schedulers to overbook dial-in participants

1. Go to Admin > Conference Settings.
2. In the Allow Overbooking of dial-in participants section of the Conference Settings page, check the Enabled check box.
3. Click Update.

Add Customized Text to E-mail Notifications

To add customized text to all conferencing E-mail notifications

1. Go to Admin > Server Settings > E-mail.
2. In the Text at the Beginning of the Reminder E-mail section of the E-mail page, type in the introductory text you want to appear at the start of all conferencing E-mail notifications.
   This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.
3. In the Text at the End of the Reminder E-mail section of the E-mail page, type in the closing text you want to appear at the end of all conferencing E-mail notifications.
   This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.
4. Click Update.
Edit Customized Text in E-mail Notifications

To edit the customized text in all conferencing E-mail notifications

1. Go to Admin > Server Settings > E-mail.

2. To change the introductory text, replace the text in the Text at the Beginning of the Reminder E-mail section of the E-mail page with the new text you want to appear at the start of all conferencing E-mail notifications.

   This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.

3. To change the closing text, replace the text in the Text at the End of the Reminder E-mail section of the E-mail page with the new text you want to appear at the end of all conferencing E-mail notifications.

   This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.

4. Click Update.

Delete Customized Text in E-mail Notifications

To delete the customized text in all conferencing E-mail notifications

1. Go to Admin > Server Settings > E-mail.

2. To delete the introductory text, select the text in the Text at the Beginning of the Reminder E-mail section of the E-mail page and press DELETE.

3. To delete the closing text, select the text in the Text at the End of the Reminder E-mail section of the E-mail page and press DELETE.

4. Click Update.
Managing Meeting Rooms

This chapter describes how to set up rooms in the Polycom® RealPresence® Resource Manager system. It includes these topics:

- “Local and Enterprise Meeting Rooms” on page 355
- “View the Rooms List” on page 356
- “Add a Local Room” on page 356
- “Add an Enterprise Room” on page 358
- “Edit a Room” on page 359
- “Delete a Room” on page 359

Local and Enterprise Meeting Rooms

The RealPresence Resource Manager system allows a user assigned the default Administrator role or the Area Administrator role to manage local and enterprise meeting rooms and the endpoints associated with those meeting rooms.

Most often a system is integrated with an enterprise directory to which rooms have been added. However, the system also allows you to add local rooms (that is, rooms added manually to the system) and associate them with endpoints.

If you want to dynamically manage the endpoint associated with a room, you must also associate each room in the system with a machine account. The machine account allows the room’s endpoint to connect and authenticate with the system for directory and dynamic management purposes without using the endpoint user’s account. After you add a room, you can create the machine account and associate the room with the machine account. For more information, see “Add Machine Accounts” on page 462.
View the Rooms List

**To view the Rooms list**

>> Go to Admin > Rooms.

The Rooms list appears. It can be filtered by Site.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room Name</td>
<td>The unique and required name of the room.</td>
</tr>
<tr>
<td>Description</td>
<td>The optional description of the room.</td>
</tr>
<tr>
<td>Site</td>
<td>The location of the room as identified in the site topology.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When areas are enabled on your system, this field shows a value of Restricted if you do not have permission to manage the area to which the site is assigned.</td>
</tr>
<tr>
<td>Associated Endpoints</td>
<td>The primary endpoint associated with this room. A set of ellipses (...) indicates the room has more than one associated endpoint.</td>
</tr>
<tr>
<td>Selected Area</td>
<td>The area to which this room is assigned.</td>
</tr>
<tr>
<td></td>
<td>This field is only visible when Areas are enabled.</td>
</tr>
<tr>
<td></td>
<td>A user can only view area-specific information for an area(s) that he has permission to manage.</td>
</tr>
</tbody>
</table>

Add a Local Room

When you add a local room to your system, you specify room settings and associate one or more endpoints with the room.

**Note for Dynamically Managed Endpoints Associated with Rooms**

If you want to dynamically manage the endpoint associated with a room, you must also associate the room with a machine account. The machine account allows the room’s endpoint to connect and authenticate with the system for directory and dynamic management purposes without using the endpoint user’s account.

After you add a room, you can create the machine account and associate the room with the machine account. For more information, see “Add Machine Accounts” on page 462.
To add a local room

1. Go to Admin > Rooms.
2. On the Rooms page, click Add. The Add New Room dialog box appears.
3. If you are logged into a domain other than the Local domain, click Manually Define.
4. Complete the General Info and Associated Endpoints sections of the Add New Room dialog box. The following table shows the room information in the RealPresence Resource Manager system records.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Room Name</td>
<td>The name of the room, which appears in the address book for associated endpoints.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A useful description (ASCII only) of the room.</td>
</tr>
<tr>
<td>Site</td>
<td>The site in which the room is located.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rooms and the endpoint associated with them must be assigned to the same site.</td>
</tr>
<tr>
<td></td>
<td>• When areas are enabled on your system, this field shows a value of Restricted if you do not have permission to manage the area to which the site is assigned.</td>
</tr>
<tr>
<td>Email</td>
<td>(Optional) The E-mail address of the room administrator.</td>
</tr>
<tr>
<td>Assign Area</td>
<td>Select an area to which to assign this room. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.</td>
</tr>
<tr>
<td><strong>Associated Endpoints</strong></td>
<td></td>
</tr>
<tr>
<td>Available Endpoints</td>
<td>The list of unassigned endpoints that are managed by the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Selected Endpoints</td>
<td>The list of endpoints assigned to the room. The endpoint at the top of the list is the primary endpoint. You can change the order of endpoint priority by selecting a endpoint and clicking Move Up or Move Down.</td>
</tr>
</tbody>
</table>
In the **Dial String Reservations** section, select the room’s **Device** and enter the appropriate dial strings for **SIP URI**, **E164**, and **H323 ID**. Click **Apply** to view the dial strings in the table below.

If the room has multiple endpoints, enter the dial strings for one endpoint type at a time and click **Apply** each time.

Click **OK**.

The room is added to the system. Note that the system does not distinguish between enterprise rooms and local rooms once they’ve been added to the system.

**Add an Enterprise Room**

If your system is integrated with an enterprise directory, you can add a room from the enterprise directory to the system.

**Note for Dynamically Managed Endpoints Associated with Rooms**

If you want to dynamically manage the endpoint associated with a room, you must also associate the room with a machine account. The machine account allows the room’s endpoint to connect and authenticate with the system for directory and dynamic management purposes without using the endpoint user’s account.

After you add a room, you can create the machine account and associate the room with the machine account. For more information, see “Add Machine Accounts” on page 462.

**To add an enterprise room**

1. Go to **Admin > Rooms**.

2. On the **Rooms** list, click **Add Room**.

   The **Add New Room** dialog box appears.

3. To find a room in the enterprise directory:
   a. In the **Search Value** field, type in the first few characters of the room name.

      The system does a prefix search of the appropriate fields.

   b. Click **Search**.

      A list of the enterprise users and rooms that meet the search criteria appears. If the search found more than 500 matching entries, only the first 500 are displayed.

   c. Select the room of interest and click **Define Details**.
4 Complete the **General Info**, **Associated Devices**, and **Dial String Reservations** sections of the **Add New Room** dialog box. For information on these fields, see “Add a Local Room” on page 356.

5 Click **OK**.

The room is added to the system. Note that the system does not distinguish between enterprise rooms and local rooms once they’ve been added to the system.

### Edit a Room

**To edit a room**

1 Go to **Admin > Rooms**.
2 In the **Rooms** list, select the room of interest and click **Edit**.
3 Edit the **General Info**, **Associated Devices**, and **Dial String Reservations** sections of the **Edit Room** dialog box. For information on these fields, see “Add a Local Room” on page 356.
4 Click **OK**.

### Note for Dynamically Managed Endpoints Associated with Rooms

If you want to dynamically manage the endpoint associated with a room, you must also associate the room with a machine account. The machine account allows the room’s endpoint to connect and authenticate with the system for directory and dynamic management purposes without using the endpoint user’s account. After you add a room, you can create the machine account and associate the room with the machine account. For more information, see “Add Machine Accounts” on page 462.

### Delete a Room

**To delete a room**

1 Go to **Admin > Rooms**.
2 In the **Rooms** list, select the room of interest and click **Delete**.
3 In the **Delete Room** dialog box, click **Yes**.

The room is deleted from the RealPresence Resource Manager system.
This chapter describes the Polycom® RealPresence® Resource Manager system enterprise directory integration and operations. It includes these topics:

- “Directory Management Overview” on page 361
- “Directory Management Supported Configurations” on page 362
- “RealPresence Resource Manager System and Windows Authentication” on page 368
- “Managing Directories” on page 370
- “Endpoint Directory and Directory Settings” on page 375

**Directory Management Overview**

In a large organization, integrating your RealPresence Resource Manager system with Microsoft Active Directory greatly simplifies the task of managing conference system security. Directory management provides the following features.

- Single sign-on capability. Users get the benefits of pass-through authentication, allowing them to leverage their Active Directory user name and password to login to the Polycom CMA Desktop system. This happens without the user having to enter their credentials, creating seamless integration for logins.

- Single management environment. After the initial setup of the RealPresence Resource Manager system, adding groups into RealPresence Resource Manager system is no more complex than adding a group to a file share or database. Continue to manage your group memberships through Active Directory, then grant those groups rights within the RealPresence Resource Manager system.

- Allows you to continue leveraging the existing role-based security model that you have in place, though the RealPresence Resource Manager system only uses Universal groups.
Directory Management Supported Configurations

There are many possible configurations available within Microsoft Active Directory, some of which are not fully supported by the RealPresence Resource Manager system. These topics describe the implications of different Microsoft Active Directory configurations for integrating with the RealPresence Resource Manager system.

Multiple Forests

Microsoft Active Directory may be set up in either a single-forest or multi-forest configuration. However, the RealPresence Resource Manager system requires that user accounts reside in a single forest.

Multiple Domains

Microsoft Active Directory forests may contain one or more domains. In either configuration, the directory must have a Global Catalog service. The RealPresence Resource Manager system can integrate to either single or multiple domains, so long as they reside in the same forest structure.

Microsoft Active Directory domains are organized into trees, each tree being a group of domains which share a consistent DNS namespace (ex: polycom.com and na.polycom.com would be in the same tree, while polycom.com and resourceManagerDevelopment.net would be separate trees, if they were in the same forest). The RealPresence Resource Manager system will integrate to all domains in a multi-tree forest.

Viable options:

1. Integrate to all domains of a multi-domain forest configuration.
2. Restrict to a single domain tree in a multi-domain forest through the use of LDAP Search baseDN criteria.

Groups

Microsoft Active Directory provides three group scopes: Universal, Global, and Domain Local. Both Global groups and Universal Groups are held on all Global Catalog servers in the forest. The RealPresence Resource Manager system supports only the Universal groups.

Microsoft Active Directory provides two group types: Security and Distribution. The RealPresence Resource Manager system supports either of these group types.
In addition to leveraging Active Directory Universal groups, the RealPresence Resource Manager system also has Local groups, which you can use to grant a standard set of rights to multiple users or groups. These RealPresence Resource Manager system Local groups can have as members, RealPresence Resource Manager system Local users, Active Directory users or Active Directory Universal groups. In this fashion, you can nest a variety of users and groups into a RealPresence Resource Manager system Local group and assign those users rights through their RealPresence Resource Manager system Local group membership, simplifying management of rights on the RealPresence Resource Manager system.

**Users**

The RealPresence Resource Manager system supports both local and enterprise user accounts. Local user accounts exist entirely on the RealPresence Resource Manager system. They can be created and managed whether or not the system is integrated to an enterprise directory. Enterprise user accounts exist in your enterprise Active Directory. The RealPresence Resource Manager system cannot create or manage Active Directory accounts, except to modify their privileges on the RealPresence Resource Manager system itself.

If simultaneously using local and enterprise accounts, it is important to avoid duplication of account data. For example, if your Active Directory has a user named John Doe with a username of jdoe, a local account for this user must possess a unique name, such as localjdoe or johndoetest. If duplicate user accounts exist in the same domain or across domains, the user associated with these accounts will not be able to log into a dynamically managed endpoint.

The RealPresence Resource Manager system accesses the enterprise directory in a read-only mode. It does not create, modify, or delete Active Directory users or groups in any way.

Once you integrate with an enterprise directory, it’s best to minimize your dependency on local users. A single local administrative user account must exist, and it should be used only when there is a problem connecting to the enterprise directory.

This configuration provides flexibility and varying security levels as follows:

- **Restricted access:** For security reasons, local user accounts do not have access to any data in Active Directory, though they can see the Active Directory users and groups as defined in the RealPresence Resource Manager system’s security.
• Administration: Active Directory users and their Active Directory group memberships are managed through your Active Directory. RealPresence Resource Manager system local users are managed through the RealPresence Resource Manager system’s web interface.

• Security: Local accounts have their own passwords, which are stored on the RealPresence Resource Manager system. Active Directory user accounts maintain the same users' Active Directory credentials and password complexity policies, which are validated by the domain controllers.

How Global Catalog Searches Work

When you integrate the RealPresence Resource Manager system with Active Directory, you can configure it to integrate in one of two ways:

• It can access a specific global catalog server by host name or IP address (not recommended, due to a lack of redundancy).

  If you select this option, the domain name that you specify for the RealPresence Resource Manager system must match the DNS name suffix of the Global Catalog server (example: dc1.polycom.com configured as the Global Catalog, then you must enter polycom.com as the domain name of the RealPresence Resource Manager system server).

• It can auto-discover the server by querying the DNS for the closest Global Catalog server (strongly recommended).

  If you select this option, you can specify any domain in the Active Directory forest in the Domain Name criteria for the RealPresence Resource Manager system server. The DNS server must contain Active Directory-specific entries.

  It is recommended that you enter the forest root DNS domain name.

When configured to auto-discover the server, every time the RealPresence Resource Manager system needs to bind to a Global Catalog server for LDAP queries, the RealPresence Resource Manager system performs the following:

• Uses Microsoft’s LDAP Ping mechanism to determine the site in which the system is located.

• Uses a DNS SRV record query to find a Global Catalog server within the same site.

• Connects to the Global Catalog on the domain controller and queries for the object in question and any relevant information (such as GUID, userID, name, phone number).

You can secure the connection between the RealPresence Resource Manager system and the Active Directory server's Global Catalog using LDAP-S (via outbound TCP/UDP port 3269) or Start TLS (via outbound 3268 TCP/UDP). To implement the secure connection, the appropriate ports must be open on any network equipment between the Global Catalog and the RealPresence Resource Manager system.
Accounts Required for the System

**RealPresence Resource Manager System Service Account**

Before integrating the RealPresence Resource Manager system with an Active Directory forest, you must create a service account for it in Active Directory. This service account is a read-only user account that the RealPresence Resource Manager system uses to perform LDAP queries against your Active Directory Global Catalog.

**RealPresence Resource Manager System Computer Account**

The RealPresence Resource Manager system requires a computer account to enable secure channel communications with the Active Directory forest that is being leveraged for authentication. This account must be pre-created and the password set by an administrator from a Domain Controller.

When setting up a redundant RealPresence Resource Manager system, the redundant servers use the same computer account to create their secure channel connection. The computer account name does not have to match the host name of your RealPresence Resource Manager system server.

**Understanding Base DN**

When the RealPresence Resource Manager system is integrated with an enterprise directory, the system uses the base DN to determine domains and manage directory searches.

The Base DN field is where you specify the distinguished name (DN) of a subset of the Active Directory hierarchy (a domain, subset of domains, or organizational unit) to which you want to restrict the RealPresence Resource Manager system search. It acts like a filter.

By default, the Base DN field is empty. The first time you tell the system to connect to the enterprise directory server, leave the Base DN field empty. Once you have established a working connection with your Active Directory, then you enter a Base DN.
The following table illustrates some basic examples of Base DN filter expressions.

<table>
<thead>
<tr>
<th>Search baseDN expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ou=ResourceManagerGroups,dc=example,dc=com)</td>
<td>Include only groups and users which reside within the ResourceManagerGroups OU in the example.com domain.</td>
</tr>
<tr>
<td>(dc=example,dc=com)</td>
<td>Include only groups and users which reside within the example.com domain or domain tree.</td>
</tr>
</tbody>
</table>

Expressions in the Base DN and exclusion filter fields must be formatted according to RFC-4514, section 2.4.

Some special characters are allowed in the BaseDN field. They include:

<table>
<thead>
<tr>
<th>Character</th>
<th>Character Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>“ % ”</td>
<td>Percent</td>
</tr>
<tr>
<td>“ * ”</td>
<td>Space</td>
</tr>
<tr>
<td>“ ”</td>
<td>Double quote</td>
</tr>
<tr>
<td>“ ? ”</td>
<td>Question mark</td>
</tr>
<tr>
<td>“ { “</td>
<td>Open brace</td>
</tr>
<tr>
<td>“ ] “</td>
<td>Close brace</td>
</tr>
<tr>
<td>“ ^ “</td>
<td>Caret</td>
</tr>
<tr>
<td>“ ~ ”</td>
<td>Tilde</td>
</tr>
<tr>
<td>“ [ “</td>
<td>Open bracket</td>
</tr>
<tr>
<td>“ ] “</td>
<td>Close bracket</td>
</tr>
<tr>
<td>“ : “</td>
<td>Single quote</td>
</tr>
<tr>
<td>“ &amp; “</td>
<td>Ampersand</td>
</tr>
<tr>
<td>“</td>
<td>Pipe or bar</td>
</tr>
</tbody>
</table>
The special characters that are not allowed in the **Base DN** field without the special escape character (backslash, \\) are:

<table>
<thead>
<tr>
<th>Character</th>
<th>Character Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot; \ &quot;</td>
<td>Backslash</td>
</tr>
<tr>
<td>&quot; = &quot;</td>
<td>Equal</td>
</tr>
<tr>
<td>&quot; , &quot;</td>
<td>Comma</td>
</tr>
<tr>
<td>&quot; # &quot;</td>
<td>Pound</td>
</tr>
<tr>
<td>&quot; + &quot;</td>
<td>Plus</td>
</tr>
<tr>
<td>&quot; : &quot;</td>
<td>Semicolon</td>
</tr>
<tr>
<td>&quot; &lt; &quot;</td>
<td>Less than</td>
</tr>
<tr>
<td>&quot; &gt; &quot;</td>
<td>Greater than</td>
</tr>
</tbody>
</table>

Therefore, to use these character as part of a name, they must be preceded in the **Base DN** field by a backslash. For example, the baseDN of an ou named "tom,ann,bob" in the "myteam.example.com" domain must be entered as:

```plaintext
ou=tom\\,ann\\,bob\\ dc=my team,dc=example,dc=com
```

Or the baseDN of an ou named "#+,=<>\ " in the "mydomain.example.com" domain must be entered as:

```plaintext
ou=\#+,=<>\ dc=mydomain,dc=example,dc=com
```

Note that this applies only to attribute values, not the ou= or dc= structure.

### Understanding Exclusion Filters

Using LDAP exclusion filters, you can exclude objects in your directory based on a wide variety of criteria within your Active Directory environment. Any LDAP filters that you create must follow the LDAP standard and reference the LDAP display name of the attributes against which you are filtering.

The following table illustrates some basic examples of exclusion filter expressions.

<table>
<thead>
<tr>
<th>Search baseDN expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memberof=cn=Restricted Group,OU=users,dc=example,dc=com</td>
<td>Excludes all users who are members of &quot;Restricted Group&quot; within the Users OU in the example.com domain.</td>
</tr>
<tr>
<td>!(Memberof=cn=Video Users,OU=Users,dc=example,dc=com)</td>
<td>Includes only groups and users within the Video Users group in the Users OU in the example.com domain.</td>
</tr>
</tbody>
</table>
Creating exclusion filters can impact the performance of your LDAP queries. As a best practice, use indexed attributes and do not use medial searches when implementing exclusion filters. For more information, see Creating More Efficient Microsoft Active Directory-Enabled Applications.

The following table illustrates some more advanced examples of exclusion filter expressions.

<table>
<thead>
<tr>
<th>Search baseDN expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!(</td>
<td>(memberof=CN=Sales,DC=europe,DC=example,DC=com) (memberof=CN=IT,DC=europe,DC=example,DC=com))</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
<td>• The expression should be in continuous line with no carriage returns or extra spaces (not possible in this document’s format).</td>
</tr>
<tr>
<td></td>
<td>• By excluding an entity, we implicitly mean to include all other entities. Conversely, by including an entity, we are implicitly excluding all other entities. Hence, this exclusion filter will suffice for a case where, for example, the administrator wants to include Sales and IT but exclude Human Resources, Engineering, etc., within the specified domain.</td>
</tr>
<tr>
<td>&amp;(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2)</td>
<td>Excludes all users who are disabled. Note this is using a different but valid notation.</td>
</tr>
</tbody>
</table>

**RealPresence Resource Manager System and Windows Authentication**

To allow Microsoft Active Directory users with dynamically-managed endpoints to securely log into their endpoint without typing in their network credentials, the RealPresence Resource Manager system must be integrated with an Active Directory server and trusted by Active Directory.

When the RealPresence Resource Manager system starts up, it performs the following actions.

• Uses Microsoft’s LDAP ping mechanism to determine the site in which the system is located.

• Uses a DNS SRV record query to find a domain controller within the same site.
When an Active Directory user attempts to log into the RealPresence Resource Manager system, it authenticates the user by connecting to the domain controller that it is connected to and passes the user's credentials using NTLMv2. The credentials are seamlessly passed to the RealPresence Resource Manager system utilizing a secure channel connection from the user’s workstation, using the credentials with which they logged into the workstation.

Because the RealPresence Resource Manager system uses NTLMv2, the password is not stored within and the RealPresence Resource Manager system never receives the user's password.

Some important notes about the RealPresence Resource Manager system Active Directory integration:

- The RealPresence Resource Manager system is not joined to the domain. Other computers on the network cannot browse its file system and it cannot be managed remotely by existing IT mechanisms such as SMS.
- The RealPresence Resource Manager system does not modify the Active Directory in any way.
- The RealPresence Resource Manager system can auto-discover the closest logical domain controller and Active Directory servers, but to do this the network DNS server must have a DNS SRV record for these servers. Once the domain controller’s hostname and IP address have a record on the DNS, the RealPresence Resource Manager system can auto-discover the IP address of the domain controller. If your Active Directory does not publish the domain controller's hostname and IP address to the network DNS, you must edit the file to include it.
- The RealPresence Resource Manager system requires that you enable Digitally sign communications on the Active Directory server.

**Generating E.164 Aliases**

The RealPresence Resource Manager system generates E.164 aliases for registered endpoints. The alias it creates is based on the endpoint type, so that a single user with multiple endpoints can have multiple E.164 aliases.

**Polycom CMA Desktop Clients**

When a user of a CMA Desktop client successfully logs into a RealPresence Resource Manager system, the RealPresence Resource Manager system creates an E.164 alias for that client. This alias is based on the user's phone number in Active Directory (or a random, unique number, if no phone number is listed for the user). Users of other endpoints can connect to the user's endpoint by dialing this alias or by searching for them by name in the directory.
Polycom HDX Systems

When a user of a Polycom HDX system successfully logs into a RealPresence Resource Manager system, the RealPresence Resource Manager system creates an E.164 alias for that endpoint also. Again, this alias is based on the user’s phone number in Active Directory (or a random, unique number, if no phone number is listed for the user), but with a “1” appended to the number. Users of other endpoints can connect to the user’s endpoint by dialing this alias or by searching for them by name in the directory.

Polycom VVX Systems

When a user of a Polycom VVX system successfully logs into a RealPresence Resource Manager system, the RealPresence Resource Manager system creates an E.164 alias for that endpoint also. Again, this alias is based on the user’s phone number in Active Directory (or a random, unique number, if no phone number is listed for the user), but with a “2” appended to the number. Users of other endpoints can connect to the user’s endpoint by dialing this alias or by searching for them by name in the directory.

Managing Directories

This section describe the directory management operations. It includes these topics:

• “Integrate with Enterprise Directory Server Option” on page 370
• “Allow Delegated Authentication to Enterprise Directory Server” on page 374
• “Remove or Include Dynamically-Managed Endpoints in the Global Address Book” on page 376

Integrate with Enterprise Directory Server Option

The process of integrating with an enterprise directory server, involves these steps:

• “Create the RealPresence Resource Manager System Service Account” on page 371
• “Create the RealPresence Resource Manager System Computer Account” on page 372
• “Enable Integration with the Enterprise Directory Server” on page 373

Enabling the Integrate with Enterprise Directory Server option allows RealPresence Resource Manager system users who are included in the Active Directory to log into the RealPresence Resource Manager system interface using their network credentials.
Enabling the **Integrate with Enterprise Directory Server** option also allows endpoint users to select conference participants and rooms from the enterprise directory. Because endpoint connections to LDAP use the endpoint user’s credentials, the Active Directory access control lists identify which endpoint users and rooms each user can see.

The RealPresence Resource Manager system supports only the Microsoft Active Directory for its enterprise directory.

In addition, administrative users can:

- View some enterprise user and group information
- Import enterprise groups into the RealPresence Resource Manager system
- Assign roles to users in different enterprise groups
- Identify enterprise resources, such as rooms, so that they can be treated as resources in the RealPresence Resource Manager system

To allow endpoint users to use NTLM Single Sign On technology to connect to the RealPresence Resource Manager system and access services such as automatic provisioning, automatic software update, and presence, see "Allow Delegated Authentication to Enterprise Directory Server" on page 374.

For more information about Active Directory and LDAP, see MS Strategy for Lightweight Directory Access Protocol (LDAP).

**Create the RealPresence Resource Manager System Service Account**

To create the RealPresence Resource Manager system service account

1. On the Active Directory server, open the **Active Directory Users and Computers** module (Start > Programs > Administrative Tools > Active Directory Users and Computers).

2. Click the node for your domain and then right-click the OU folder in which you want to add a user account and select **New > User**.

3. At a minimum, in the First name, Full name, and User logon name fields, type resourcemanservice or an appropriate name for your environment and click **Next**.

4. In the Password and Confirm Password fields, type a password for the service account to use during initial integration. This is the password you must enter on the RealPresence Resource Manager system **Enterprise Server** page.
5 Select the **Password never expires** option, unselect the **User cannot change password** option, click **Next** and then **Finish**.

- You can reset the password for this account manually, but to do so you must change it in Active Directory first and then update the RealPresence Resource Manager system LDAP Server page.
- The service account requires the rights to read all properties on all users and groups that will be used in the RealPresence Resource Manager system. Without these permissions, it may not function properly.

---

**Create the RealPresence Resource Manager System Computer Account**

**To create the RealPresence Resource Manager System computer account**

1. On the Microsoft Active Directory system, open the **Active Directory Users and Computers** module (Start > Programs > Administrative Tools > Active Directory Users and Computers).
2. Select the node for your domain, right-click the OU folder in which to add the computer account and then select **New > Computer**.
3. In the **Computer name** field, type **PolycomResourceManager** or an appropriate name for your environment and then click **Next** and **Finish** (or simply click **OK** depending on your version of Active Directory).
4. Ensure that the **Active Directory Users and Computers** console will show all available computer options necessary for the remaining steps by enabling **View > Advanced Features**.
5. Right-click the computer account, select **Properties**, and then select the **Security** tab.
6. In the **Group or user names** section of the Security tab, select the **SELF** object.
7. In the **Permissions for SELF** section, select **Change password**, and then click **OK**.
8. Login to the domain controller where the computer account was created and set the password using the following command:

   `net user <computername>$ <password>`

   For example: `net user polycomresoucemanager$ p@ssW0rd`
Performing the net user command on any machine other than a domain controller will not assign the computer account password for the RealPresence Resource Manager system computer account.

At initial integration, the RealPresence Resource Manager system will change its Computer Account password to a random 120 character string including special characters. This password will also be changed, to a new randomly generated password, every time the RealPresence Resource Manager system is rebooted, or every week if no reboots are performed. Because this is a Computer account, resetting the password to a known value requires use of net user commands on an Active Directory Domain Controller.

Enable Integration with the Enterprise Directory Server

To integrate the RealPresence Resource Manager system to an enterprise directory server

1. Go to Admin > Directories > Enterprise Directory.
3. To have the system auto-discover the server by querying DNS, enable Auto-discover in the Enterprise Directory Server DNS Name section; otherwise, enter the DNS Name for the enterprise directory server.
4. As needed, configure these settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain\Enterprise Directory User ID</td>
<td>Domain and Enterprise Directory User ID for an account that the RealPresence Resource Manager system can use to access the enterprise directory server and retrieve group, user, and room information. This is the account created “Create the RealPresence Resource Manager System Service Account” on page 371. This User ID must have read permissions so it can search the entire forest on the enterprise directory server. This User ID is automatically associated with the RealPresence Resource Manager system administrator role - by default it is the ONLY enterprise directory User ID with this role.</td>
</tr>
<tr>
<td>Enterprise Directory User Password</td>
<td>The password for the enterprise directory user account</td>
</tr>
</tbody>
</table>
If you also wish to implement single sign-on, see the following section “Allow Delegated Authentication to Enterprise Directory Server” on page 374. Otherwise, click Update.

### Allow Delegated Authentication to Enterprise Directory Server

The RealPresence Resource Manager system Use Single Sign on (Integrated Windows Authentication) option, allows endpoint users who are included in the enterprise directory to securely log into their dynamically-managed endpoint without typing in credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level</td>
<td>The level of security on the connection between the RealPresence Resource Manager system and the enterprise directory server. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Plain—No security on the connection</td>
</tr>
</tbody>
</table>
|                                  | • LDAPS—The connection is secured over outbound port 3269 using LDAP-S in a manner similar to https.  
  If the “Domain Controller: LDAP Server signing requirements” setting on the Active Directory server is set to “Require Signing”, then you must use LDAPS to secure the connection.                                                                                                   |
|                                  | • StartTLS—The connection is secured over outbound port 3268 (the same port as Plain), but it then negotiates security once the socket is opened. Some LDAP servers reject any unsecured transactions, so the first command is the StartTLS negotiation command.                                                                                                      |
| Ignore Disabled Enterprise Directory Users | Check this field to have the RealPresence Resource Manager system ignore disabled enterprise users in its queries.                                                                                                                                                                                                                          |
| Enterprise Directory Exclusion Filter | If necessary and you understand the filter syntax, specify other types of user accounts to exclude. Don’t edit these expressions unless you understand LDAP filter syntax. For more information, see “Understanding Exclusion Filters” on page 367.                                                                 |
| Enterprise Directory Search BaseDN | If necessary and you understand the filter syntax, specify the top level of the enterprise directory tree (referred to as the base DN) to search. Don’t edit these expressions unless you understand the filter syntax. For more information, see “Understanding Base DN” on page 365. |
To delegate authentication to the enterprise directory server

1. Go to Admin > Directories > Enterprise Directory.

2. On the Enterprise Directory page, select Allow delegated authentication to enterprise directory server.

3. To have the system auto-discover the closest logical domain controller and enterprise directory servers, in the Domain controller name section enable Auto-discover; otherwise, enter the fully qualified hostname of the domain controller (for example, dc1.mydomain.com).

4. Enter the Username (domain\computer name) and Password and click Update.

Endpoint Directory and Directory Settings

When an endpoint registers with the RealPresence Resource Manager system, its information is automatically entered into the Global Address Book. When information changes at the endpoint, the Global Address Book is automatically updated as well. If an endpoint is configured to Allow Directory Changes, additions and deletions to the Global Address Book are pushed to the endpoint.

Endpoints that get their global directory from the RealPresence Resource Manager system will either get the Global Address Book or the enterprise LDAP directory. Two Directory Setup options allow you to affect which devices and users appear in the endpoint directory.

Typically, standard endpoints (those that are not dynamically managed) register for the Polycom GDS and are listed in the RealPresence Resource Manager system Global Address Book. The Global Address Book allows standard endpoint users to call other standard endpoint users by selecting them by name. In this case, the Global Address Book is limited to 2000 entries, which is the limit that standard endpoint systems can manage.
The **Include dynamically-managed devices in the Global Address Book** option changes the Global Address Book so that it includes all standard endpoints and all dynamically-managed endpoints such as CMA Desktop and Polycom VVX 1500 endpoints in the Global Address Book. In this case, the Global Address Book limit is increased to 5000 entries. (Dynamically-managed endpoints are always included in the enterprise LDAP directory.)

By default the **Include dynamically-managed devices in the Global Address Book** option is selected. This brings all of your devices and users together into one endpoint directory. However, you may not want to take advantage of this feature if you have legacy endpoint systems such as VSX and FX endpoints. These endpoint systems cannot handle the increased size of the Global Address Book. For information on clearing this option, see “Remove or Include Dynamically-Managed Endpoints in the Global Address Book” on page 376.

The second **Directory Setup** option affects both the Global Address Book and the enterprise LDAP directory. The RealPresence Resource Manager system Guest Book includes static user entries. By selecting the **Show Guest Book entries in the Directory**, these static entries are included in the endpoint directory, regardless of whether the endpoint directory is the Global Address Book or the enterprise LDAP directory. The **Show Guest Book entries in the Directory** option is also selected by default.

### Remove or Include Dynamically-Managed Endpoints in the Global Address Book

By default the RealPresence Resource Manager system includes dynamically-managed endpoints in the Global Address Book. However, you may not want to take advantage of this feature if you have legacy endpoints such as VSX and FX endpoints. These endpoints may not be able to handle the increased size of the Global Address Book.

**To remove enterprise users from the RealPresence Resource Manager system Global Address Book**

1. Go to **Admin > Directories > Directory Setup**.
2 In the Directory page, clear Include dynamically-managed devices in the Global Address Book.

3 Click Update.

To include enterprise users in the RealPresence Resource Manager system Global Address Book
1 Go to Admin > Directories > Directory Setup.
2 In the Directory page, select Include dynamically-managed devices in the Global Address Book.
3 Click Update.

Remove or Include Guest Book Entries in the Directory

By default the RealPresence Resource Manager system includes Guest Book entries in the endpoint directory, regardless of whether the endpoint directory is the Global Address Book or the enterprise directory.

To remove Guest Book entries from the endpoint directory
1 Go to Admin > Directories > Directory Setup.
2 In the Directory Setup page, clear Show Guest Book entries in the Directory.
3 Click Update.

To include Guest Book entries in the endpoint directory
1 Go to Admin > Directories > Directory Setup.
2 In the Directory Setup page, select Show Guest Book entries in the Directory.
3 Click Update.

Allow Local Users to View Enterprise Directory Entries

You can allow local users to access Enterprise Directory entries when the RealPresence Resource Manager is integrated with an enterprise directory.

To allow local users to view Enterprise Directory Entries
1 Go to Admin > Directories > Directory Setup.
2 In the Directory Setup page, mark the Allow endpoint directories for local users to include enterprise directory user information check box.
Support LifeSize Endpoints in Directories

You can include LifeSize endpoints in the endpoint directory by configuring your directory setup. When you do this, you also need to ensure that your LifeSize endpoint is configured to use the correct LDAP settings.

Complete the following steps:

- “Modify Directory Listings” on page 378
- “Configure LDAP Settings” on page 378

For more information about LifeSize endpoints, see “Considerations for LifeSize Endpoints” on page 184.

Modify Directory Listings

You need to allow your directory listings to include support for LifeSize endpoints.

To modify directory listings for LifeSize endpoint support

2. In the Directory Setup page, mark the Modify directory listings for LifeSize endpoint support check box.
3. Click Update.

Configure LDAP Settings

In addition to configuring directory listing support in the directory set up, you need to also ensure that the LifeSize endpoint is configured to use the RealPresence Resource Manager system’s LDAP settings. You can provision these through a scheduled provisioning profile or configure them manually on the endpoint.

To add LDAP settings to a scheduled provisioning profile

1. Go to Admin > Provisioning Profiles > Scheduled Provisioning Profiles.
2. In the Scheduled Provisioning Profiles page, click Add.
3. In the Add Profile dialog box, select the Endpoint Type for the provisioning profile, enter a name for the profile, and click Next.
4 As needed, complete the various settings that you would like to provision for your LifeSize endpoint.

For more information about these fields, see “Endpoint Fields for Scheduled Provisioning” on page 196.

5 For Directory support, select the Directory > LDAP page.

6 On the Directory > LDAP page:
   a Mark the Provision This Page check box.
   b In the LDAP field, select Enabled from the drop-down list.
      » In the LDAP Username field, enter uid=ldapgab,ou=system
      » In the LDAP Password field, enter the password for the Polycom Global Address Book if you have one. If not, leave this field blank.
      » In the LDAP Base field, enter DC=Polycom,dc=com

7 Click OK.

If you manually enter the LDAP settings on the LifeSize endpoint, the value for the LDAP Base field needs to be the following:
OU=Endpoints,DC=Polycom,dc=com.
Setting Up Directories

This chapter describes how to manage the Global Address Book in the Polycom® RealPresence® Resource Manager system. It includes these topics:

• “View the Global Address Book” on page 381
• “Set or Change the GAB Password” on page 382

View the Global Address Book

The Polycom Global Address Book is a system-managed endpoint directory that allows users with video endpoints to look up and call other users with video endpoints in their video communications network.

From a video endpoint system, users can locate other user’s endpoints by name in the Global Address Book and initiate a call without knowledge of the other user’s equipment. The RealPresence Resource Manager system will filter incompatible endpoints out of the Global Address Book (GAB) results so that the GAB presented to H.323-only endpoints will not include ISDN-only endpoints and the GAB presented to ISDN-only endpoints will not include H.323-only endpoints.

Global Address Book filtering applies only to Polycom endpoints. The Global Address Book is not filtered on third-party endpoints.

For more information on the Global Address Book, see “Endpoint Directory and Directory Settings” on page 375.

To view the Global Address Book

1 Go to Admin > Directories > Global Address Book.
2 As needed, use the Filter to customize the Global Address Book. It can be filtered by Endpoint Name, IP Address or Area.

This Area filter is only visible when Areas are enabled and the user manages more than one area. A user can only view area-specific information for an area(s) that he has permission to manage.

The user information found in the Global Address Book includes:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>The associated user or resource ID.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the registered endpoint.</td>
</tr>
<tr>
<td>GAB Display Name</td>
<td>The name of the registered endpoint as it will be displayed to other endpoint users. This display name is an ASCII only field.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the endpoint.</td>
</tr>
<tr>
<td>Alias</td>
<td>The alias associated with the endpoint.</td>
</tr>
<tr>
<td>Primary ISDN</td>
<td>The primary ISDN number for the endpoint (if any).</td>
</tr>
<tr>
<td>Secondary ISDN</td>
<td>The secondary ISDN number for the endpoint (if any).</td>
</tr>
<tr>
<td>Owner</td>
<td>The user associated with the endpoint.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the endpoint.</td>
</tr>
<tr>
<td>Area</td>
<td>The area in which the endpoint resides.</td>
</tr>
</tbody>
</table>

**Set or Change the GAB Password**

You can require that endpoints be provisioned with a password in order to access the Global Address Book on the RealPresence Resource Manager system. To do so, set a Global Address Book password as described here. Use the same procedure to change the Global Address Book password.

Note that even if the Global Address Book is password protected, some third-party endpoints may not be required to provide a password because they are not directory-password aware. They have unrestricted access to the Global Address Book.

To provision this password to endpoints, see “Add a Scheduled Provisioning Profile” on page 146.

**To set or change the password for the Global Address Book**

1 Go to Admin > Directories > Global Address Book.
2 In the **Global Address Book**, click **Set GAB Password**.

3 In the **Set Client Password** dialog box, enter the **Old Password** and the **New Password**. (Note that the password fields are ASCII only.)

4 Confirm the new password and click **Save**.

   Once you set this password, endpoints that are not provisioned with this password cannot access the Global Address Book on the RealPresence Resource Manager system.
Multiple Address Books Overview

Users assigned the Administrator role can create multiple address books in the RealPresence Resource Manager system. Multiple address books are subsets of the Global Address Book (GAB) and let you manage which users (local and enterprise), endpoints, rooms, groups, and guests appear in each address book.

Multiple address books support both the Global Address Book and LDAP protocols. Endpoints requesting directory information using either protocol receive either the default address book or the address book assigned to the user’s group.
If you do not want to use multiple address books, you can leave the default address book set to All Entries. Using this default, all users will see all entries in the directory. Be sure that all groups are assigned either the System Default or All Entries option. System Default is the default group setting.

An endpoint must be associated with a User and the User must be in a Group in order to specify an address book.

How Multiple Address Books Work

Use address books to limit access to people and endpoints. For example, you can set up separate address books for each department in your organization. Each address book would include only RealPresence Resource Manager system users in that department and only rooms in that department’s location.

Users not assigned the Administrator or Area Administrator role (available if you have enabled areas) will not be aware of address books. They will see only those users (local and enterprise directory), endpoints, rooms, groups, and guests in the same address book that the user is assigned to.

For information about how address books work in a multi-tenancy environment, see “Area Address Books” on page 401.

To implement multiple address books, complete the following tasks

1 “Add an Address Book” on page 388

RealPresence Resource Manager system users assigned the Administrator role can create address books and associate users (local and enterprise directory), endpoints, rooms, groups, and guests with one or more address books. This process controls where each entity appears as an address book entry.

2 “Assign Address Books to Groups” on page 392

RealPresence Resource Manager system users assigned the Administrator role can assign an address book to a group. A group can be assigned to only one address book. This process controls the address book that users and endpoints have access to.

3 “Change Address Book Priority” on page 394

RealPresence Resource Manager system users assigned the Administrator role can set the priority of address books. The priority affects which address book a user has access to. For example, if a user is a member of two different groups and each group is assigned a different address book, the user can access the address book that is higher in priority.
Address Book Considerations for Multi-Tenancy

If you have enabled the Areas feature, you can only associate users and endpoints that are in the same area that you have been assigned to manage.

Users not assigned the Administrator or Area Administrator role will not be aware of address books or be allowed to edit them. They will see only those users (local and enterprise directory), endpoints, rooms, groups, and guests in the same address book and area to which the user is assigned.

When you manage more than one area, you can create address books that contain users and endpoints from each area that you manage. However, users in that address book will only be able to view users from the area to which they also belong.

For more information about multi-tenancy, see “Configuring Multi-Tenancy” on page 397.

View the Address Book List and Details

To view the address book list and details

1. Go to Admin > Directories > Address Books.

The Address Book list appears, with details of the selected address book in the right pane.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The priority affects which address book a user sees. For example, if a user is a member of two different groups and each group is assigned a different address book, the user will see the address book that is higher in priority.</td>
</tr>
<tr>
<td>Address Books</td>
<td>Name of the address book.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the address book.</td>
</tr>
<tr>
<td>Area</td>
<td>This column is only available when areas have been enabled and indicates the area to which the address book belongs.</td>
</tr>
<tr>
<td></td>
<td>You can view this column if you have the administrator role or have the area administrator role and manage more than one area. If the address book belongs to an area that you do not manage, the area name will be listed as &quot;Restricted&quot; as you do not have permission to view that area.</td>
</tr>
</tbody>
</table>
2 In the **Address Book Details** in the right pane, expand the tree to view the tiers along with users, endpoints, rooms, groups, and guests associated with the address book.

### Add an Address Book

You can add many address books to the RealPresence Resource Manager system, and each address book can have up to 100 tiers.

Tiers are only meant to allow you to organize the address book contents. They will not be visible to endpoint users when they access the directory. Each tier can have up to three subtiers, and you can have address book entries at any tier level.

Associating users, endpoints, rooms, groups, and guests with an address book controls where these entities appear. For example, if you associate user A with address book A, the user will appear as an entry in address book A. You can associate any of these entities with more than one address book, and the entity will appear as entry in each address book.

Groups in the RealPresence Resource Manager system control the address book users, endpoints, and rooms have access to. To set which address book an entity has access to, see “**Assign Address Books to Groups**” on page 392.

#### To add an address book

1 Go to **Admin > Directories > Address Books**.
2 Click **Add**.
3 Complete the fields in the **Add an Address Book** dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address Book Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name to identify this address book.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the address book.</td>
</tr>
<tr>
<td>Assign Area</td>
<td>You can assign an address book to an area you manage.</td>
</tr>
<tr>
<td></td>
<td>This drop-down list is only available when areas are enabled.</td>
</tr>
<tr>
<td></td>
<td>You can only view areas that you manage.</td>
</tr>
</tbody>
</table>
4 To associate users with this address book, click **Associate Users**.

The **Address Book/Tier** column shows all of the address books the users appear in.

- a Search for the users you want to associate. Use the **Filter** to customize the list.
- b Select the users you want and click **Specify Tier**.
- c Select the tier you want for the users and click **OK**.

5 To associate endpoints with this address book, click **Associate Endpoints**.

Only endpoints that are not associated with a RealPresence Resource Manager system user appear in the list.

- a Use the **Filter** to customize the list.
  
  The **Address Book/Tier** column shows all of the address books the endpoints appear in.
- b Select the endpoints you want and click **Specify Tier**.
- c Select the tier you want for the endpoints and click **OK**.

6 To associate rooms with this address book, click **Associate Rooms**.

The **Address Book/Tier** column shows all of the address books the rooms appear in.

- a Use the **Filter** to customize the list.
- b Select the rooms you want and click **Specify Tier**.
- c Select the tier you want for the rooms and click **OK**.

7 To associate groups with this address book, click **Associate Groups**.

The **Address Book/Tier** column shows all of the address books the groups appear in.

- a Use the **Filter** to customize the list.
- b Select the groups you want and click **Specify Tier**.
- c Select the tier you want for the groups and click **OK**.
To associate guests with this address book, click **Associate Guests**.

The **Address Book/Tier** column shows all of the address books the guests appear in.

- **a** Use the **Filter** to customize the list.
- **b** Select the guests you want and click **Specify Tier**.
- **c** Select the tier you want for the guests and click **OK**.

Click **OK**.

## Edit an Address Book

You can edit an address book to add or remove users, endpoints, rooms, groups, and guests.

You can find any of these entities that are not currently associated with an address book by selecting **Current Association** from any **Filter**, then selecting **Not Associated With An Address Book**.

If a group is set up with the **Enterprise Directory Viewable** option not selected, you can still add that group to an address book. The group itself will not appear as an entry in the address book, but the members of the group will.

**To edit an address book**

1. Go to **Admin > Directories > Address Books**.
2. Select an address book.
3. Click **Edit**.
4. Edit the fields in the **Edit an Address Book** dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address Book Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name to identify this address book.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the address book.</td>
</tr>
<tr>
<td>Assign Area</td>
<td>You can assign an address book to an area you manage. This drop-down list is only available when areas are enabled. You can only view areas that you manage.</td>
</tr>
</tbody>
</table>
Using Multiple Address Books

To associate users with this address book, click **Associate Users**.

The **Address Book/Tier** column shows all of the address books the users appear in.

a. Search for the users you want to associate. Use the **Filter** to customize the list.

b. Select the users you want and click **Specify Tier**.

c. Select the tier you want for the users and click **OK**.

d. To delete a user from the address book, select the user and click **Delete**.

   The user is removed from the address book, but remains in the RealPresence Resource Manager system.

To associate endpoints with this address book, click **Associate Endpoints**.

Only endpoints that are not associated with a RealPresence Resource Manager system user appear in the list.

The **Address Book/Tier** column shows all of the address books the endpoints appear in.

a. Use the **Filter** to customize the list.

b. Select the endpoints you want and click **Specify Tier**.

c. Select the tier you want for the endpoints and click **OK**.

d. To delete an endpoint from the address book, select the endpoint and click **Delete**.

   The endpoint is removed from the address book, but remains in the RealPresence Resource Manager system.

To associate rooms with this address book, click **Associate Rooms**.

The **Address Book/Tier** column shows all of the address books the rooms appear in.

a. Use the **Filter** to customize the list.

b. Select the rooms you want and click **Specify Tier**.

c. Select the tier you want for the rooms and click **OK**.
To delete a room from the address book, select the room and click **Delete**.

The room is removed from the address book, but remains in the RealPresence Resource Manager system.

To associate groups with this address book, click **Associate Groups**.

The **Address Book/Tier** column shows all of the address books the groups appear in.

- Use the **Filter** to customize the list.
- Select the groups you want and click **Specify Tier**.
- Select the tier you want for the groups and click **OK**.
- To delete a group from the address book, select the group and click **Delete**.

The group is removed from the address book, but remains in the RealPresence Resource Manager system.

To associate guests with this address book, click **Associate Guests**.

The **Address Book/Tier** column shows all of the address books the guests appear in.

- Use the **Filter** to customize the list.
- Select the guests you want and click **Specify Tier**.
- Select the tier you want for the guests and click **OK**.
- To delete a guest from the address book, select the guest and click **Delete**.

The guest is removed from the address book, but remains in the RealPresence Resource Manager system.

Click **OK**.

### Assign Address Books to Groups

You can assign an address book to a group, but you cannot assign address books directly to users. Group assignment controls to which address book users and endpoints have access. Each group can have just one address book assigned to it, but users can be in more than one group.

Address book priority affects which address book users and endpoints can access. For example, if a user is a member of two different groups and each group is assigned a different address book, the user will see the address book that is higher in priority. To change priority, see “Change Address Book Priority” on page 394.
To assign an address book to a group

1 Go to User > Groups.
2 Select the group you want to assign.
3 Click Edit.
4 In the Edit Local Group dialog box, select address book you want from the Assign Address Book drop-down list.
5 Click OK.

Viewing the Address Book a User is Assigned To

You can see which address book a user is assigned to. The address book assignment controls the address book entries a user or endpoint can access.

To view the address book a user is assigned to

1 Go to User > Users.
2 Select the user you want.
3 Click View Details.
4 In the View User dialog box, click Inherited Group Info.
5 Click OK.

Delete an Address Book

You can delete an address book when it is no longer needed. Deleting an address book does not delete the users, endpoints, rooms, groups, or guests that were in the address from the RealPresence Resource Manager system.

Any entity that was assigned the deleted address book will have access to one of the following:

- Another address book if the entity is a member of another group that is assigned to an existing address book.
- The default address book.

To delete an address book

1 Go to Admin > Directories > Address Books.
2 Select the address book you want to delete.
3 Click Delete.
    A confirmation message appears.

4 Click Yes.

Change Address Book Priority

You can change the priority of address books. The priority determines which address book a user sees. For example, if a user is a member of two different groups and each group is associated with a different address book, the user will see the address book that is higher in priority.

The All Entries address book always has the highest priority and None always has the lowest priority. If the address book for one of the groups the user belongs to is changed to All Entries, the user will see all entries regardless of the priority of the address book for the other group.

To change address book priority
1 Go to Admin > Directories > Address Books.
2 In the Priority column of an address book, enter the priority you want.
   Use only whole numbers and only numbers that fall within the total count of address books. For example, if you have four address books, only 1 through 4 are valid priority values.
3 Click Update Priority.
   The system changes the order of the address book list.

Set the Default Address Book

You can set the default address book. The default address book sets the address book all new users have access to if no address book is assigned through a group.

If you do not want to use multiple address books in the RealPresence Resource Manager system, leave the default address book set to All Entries (the default). Using this default, all users will be able to see all entries in the directory. Be sure that all groups are assigned either the System Default or All Entries option. System Default is the default group setting.

If you create multiple address books, you can change the default address book to one of the address books you created.
To set the default address book
1. Go to Admin > Directories > Address Books.
2. Click Set Default.
3. In the Default Address Book dialog box, select the option you want:
   - All Entries — Default setting. All users, endpoints, groups, rooms, and guests are in one address book and all have access to all address book entries.
   - None — No directory entries will be available.
   - Specify — Select the address book you want as the default.
4. Click OK.

Copy an Address Book

You can copy an existing address book as a shortcut to creating a new address book. The copy process can copy the entire address book or just the tier structure.

To copy an address book
1. Go to Admin > Directories > Address Books.
2. Select the address book you want to copy.
3. Click Copy.
4. In the Copy Address Book dialog box, select the option you want:
   - Entire Address Book — This option copies all of the tiers and the users, endpoints, rooms, groups, and guests that are associated with the address book to the new address book.
     If areas are enabled, the address is copied to the same area to which the initial address book belongs.
   - Tiers only — This option copies only the tier structure to the new address book.
5. Enter a meaningful Name and Description.
6. Click OK.

You can now edit the new address book to add or delete entries.
Configuring Multi-Tenancy

The RealPresence Resource Manager system supports multi-tenancy with its areas feature. Multi-tenancy allows you to use the RealPresence Resource Manager to service multiple customers, internal or external. Each area serves a system tenant by partitioning off a collection of resources including users, associated endpoints, network devices, etc.

Administration and conferencing duties for areas can then be delegated to users within that area or by a set of super users who are allowed to view and manage all areas. You can set up flexible scenarios by having an area scheduler or area operator for each respective tenant or area. Otherwise, you can limit area administration tasks to users specifically allowed to manage that area.

For example, in an enterprise deployment, the RealPresence Resource Manager administrator can divide up users and resources according to department and then delegate video conferencing duties to users within that area. This allows the system administration duties to remain with a specialized video IT department, while video conference scheduling can be delegated to users within specific areas. Areas also allow the administrator to run area-specific reports on how specific departments within the enterprise are utilizing video conferencing.

Note
The Areas feature of the Resource Manager system is a licensed feature. Contact your sales representative for more details.

Planning For Multi-Tenancy

You should plan your multi-tenancy environment so that you can ensure scalability and efficient use of resources. Setting up the Resource Manager system for multi-tenancy should use the following best practices:

- RealPresence Resource Manager does not support integration with more than one Active Directory or multi-forest Active Directory integrations. If you need to support users that reside in different Active Directories or different Active Directory forests, you cannot use the Resource Manager
system’s integration with Active Directory feature. You will need to use only local RealPresence Resource Manager system users. To save time, you can import users into your RealPresence Resource Manager system.

- Software updates cannot be assigned to an area.
- You must use automatic provisioning when areas are enabled. Other methods of endpoint provisioning are not supported. See “Automatic Provisioning of Endpoints” on page 131
- Polycom DMA systems, Polycom VBPs, and SBCs (Acme Packet Net-Net Enterprise Session Director) are not area-aware, which means they cannot be assigned to an area.
- Resources can belong to only one area, with the exception of DMA Pool Orders. If you want to share network devices between areas, you can leave them in no area.
- You can assign an area user an area role according to the tasks the user needs to perform in the RealPresence Resource Manager. Area roles restrict user tasks to the area or areas in which they are allowed to manage.
- Some system-wide administration tasks cannot be delegated to users with only area-specific roles. These include site topology and conference templates. System maintenance and set up must also be done by a user with a system role.

Working within a Multi-Tenancy Environment

When using the RealPresence Resource Manager area feature, most aspects of the system become “area-aware” which means that management of the system and conferencing tasks may become different according to the role of the user.

The following aspects of the area feature are discussed in this topic:
- “User Roles within a Multi-Tenancy Environment” on page 398
- “Area Address Books” on page 401
- “Area User Groups” on page 401
- “Area Users, Rooms and Associated Endpoints” on page 402
- “Area Conference Guests” on page 402
- “Using the Common Pool in a Multi-Tenancy Environment” on page 402
- “Area Conference Templates” on page 402

User Roles within a Multi-Tenancy Environment

When you have enabled areas for your RealPresence Resource Manager system, you have access to additional user roles to help you delegate responsibilities to users within specific areas.
System Roles

System roles are used for users who are required to perform Resource Manager tasks for all areas. Resource Manager users that have a system role will be able to view and modify resources from all areas because their role includes the **View and/or Modify All Areas** permission.

System roles include: Administrator, Advanced Scheduler, Auditor, Device Administrator, Operator, Scheduler, and View-Only Scheduler.

For detailed information about system roles, see “Working with Management Roles and Permissions” on page 266.

Area Roles

An area role delegates Resource Manager responsibilities to a user that needs to manage the resources in one or more areas, but not all areas. A user must be assigned a RealPresence Resource Manager area role in order to perform his role-related tasks. In addition to being assigned a role, you must enable that user to manage the area(s) in which he needs to perform his responsibilities.

You can also allow a user to manage areas to which he does not belong. For example, you can allow an area scheduler to schedule users from two areas into conferences. For this, you would need to configure this user to manage both areas.

Area roles include: area administrator, area operator, and area scheduler.
Area Conference Participants

Although conferences are area-specific, an area scheduler can add users from any area that he manages.

For example, if a area scheduler for the blue area was also granted permission to manage the yellow area, he can add conference participants from both the blue and yellow areas.

A system scheduler is able to schedule conferences in all areas and invite users from all areas.

Note that if a conference has participants, rooms, and/or guests from multiple areas, then Resource Manager users will be able to see the area names of only the areas that they belong to or can manage. Participants, rooms and guests that belong to other areas are presented as a “Guest of” the conference’s area.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
</table>
| Area Scheduler     | Schedule Conferences  
|                    | Scheduling Level = Basic |
| Area Operator      | Conference operator  
|                    | Reports  
|                    | Troubleshooting  
|                    | Schedule conferences, both basic and advanced.  
|                    | Schedule-able resource monitor. The area operator can monitor MCUs and DMA Pool orders that are in the areas he manages or in the common pool (no area). |
| Area Administrator | Add endpoints.  
|                    | Manage users and groups  
|                    | Monitor conferences  
|                    | Monitor network devices  
|                    | View-only scheduler  
|                    | Directory setup  
|                    | Can provision devices using existing profiles (cannot create provisioning profiles)  
|                    | Can update software on devices using existing software updates (cannot create software updates)  
|                    | Can add and edit users, groups, rooms, and other resources.  
|                    | Can view Reports for the area(s) they manage. No system-wide reports will be available.  
|                    | Can monitor the system via the Admin Dashboard. System-wide pods will not be available. Each sub-pod will have its source information filtered by area. |
Area Address Books

An address book must belong to only one area or to no area, but can contain users, endpoints, rooms and guests from multiple areas.

An address book is accessible to only users who are also assigned to the area that the address book belongs to. That is, if a user has a system role, they will see all address books, but if a user has only an area roles, they will see only address books that belong to the areas that they belong to or to areas in which they manage.

When a user views the contents of an address book that has members from multiple areas, they will be able to view only those members that belong to areas the user has access to. That is, if a user has a non-area-specific role, they will be able to see address book members from all areas, but if a user has only area-specific roles, they will see only members that belong to the areas they manage.

From an endpoint, an address book is accessible only if the logged in user and address book belong to the same area or if the logged in user manages the area the address book belongs to. When an endpoint user views the contents of a cross-area address book, the address book members they can see include:

- Members that belong to the same area as the user who is logged in to the endpoint
- Members that belong to other areas that the logged in user manages

Also note that changing the area that an address book is assigned to does not affect the areas of its members.

Area User Groups

User groups can be assigned to one area or no area. Although it can contain users from multiple areas. Users with the system role of administrator or the role of area administrator are allowed to create and edit user groups. If the area administrator manages more than one area, he can add users from any area that he manages to the user group. Remember that system administrators are automatically have permission to view/manage all areas, and can therefore add any user to a user group.

However, even if a group has users from multiple areas, area administrators can only view users within the group that belong to the areas they manage.

Changing the area of the group does not affect the area of the users in the group.
Area Users, Rooms and Associated Endpoints

Endpoints and rooms follow strict rules of staying in the same area of the user they are associated with. The Resource Manager system ensures that a user and their associated endpoint(s) belong to the same area. If one moves to another area or no area, the others move with it. The same is true for rooms and their associated endpoints. More specifically:

- If a user or room is put into an area or moved to a different area, all of their associated endpoints will be automatically updated to the same new area.
- If one of the associated endpoints of a user or room is moved to a different area, the change will propagate to the associated user or room and any other endpoints owned by the user or room.

The logged-in user is warned that this will happen so that they can cancel the operation if this is not what they intended. The only way to move an endpoint without also moving the owner and the owner’s other endpoints is to disassociate the endpoint from the user or room before changing the area of the endpoint.

Area Conference Guests

When a new guest is added to a conference and saved to the guest book, the guest is configured to belong to the area that the conference belongs to. This area information of the guest is persisted in the guest book. If the conference’s area changes after this point, the guest’s area will not change. Users who can manage more than one area can change the guest’s area by using the editing the guest book entry.

Using the Common Pool in a Multi-Tenancy Environment

If a network device or DMA pool order does not belong to an area, it is said to be in the “common pool” and therefore is available for the system to use for any area. Any user who manages an area and has permission to perform tasks within that area can view resources that are in the common pool.

For example, an area operator can schedule a conference on an RMX system that is explicitly assigned to the area to which the operator belongs or the scheduler can use an RMX system that belongs to the common pool.

Area Conference Templates

A user must have a system administrator role in order to create new conference templates. As a best practice, the same user responsible for system set up should be responsible for creating conference templates.

Conference templates can be assigned to an specific area and also associated with users with a specific role.
As a best practice, when you create a conference template, give it an area-specific name. This is especially helpful if you allow an area scheduler to schedule conferences for more than one area.

When a scheduler (area or system) schedules a conference, he is required to use a conference template from the same area as the conference area or a template that is assigned to no area (common pool).

Configure Areas

You must configure your system for areas. Most of the configuration tasks can be completed by a user with the administrator role or area administrator role. However, network devices must be added by a user with the device administrator role.

You need to enable your system for areas and then add an area for each tenant that will use your system.

1. Enable the areas feature.
2. Add the areas that you want to use.
3. Customize the logos for each area, if desired.
4. Add network devices to areas. This task must be done by a user who has the device administrator role.
5. Import users into each area.
   This step is necessary if you need to support users who do not reside in your single LDAP directory. RealPresence Resource Manager does not support integration with multiple LDAP directories.
6. Assign roles to area users. By default, area users all have the area scheduler role. You need to determine which, if any, of the area users will be given the area administrator or area operator roles.
7. Designate which users will manage each area.
   Users must be allowed to manage an area in order to perform the tasks associated with their area role. You can allow users to manage one area, no area, multiple areas (including areas to which they do not belong).
8. Add resources to areas. This task can be done by the Resource Manager system administrator, or a user with the area administrator who is also allowed to manage the area to which he is adding endpoints/rooms.
9. Add conference templates to areas. This task needs to be done by a user with the administrator role.
10. Configure site topology.
Enable Areas

In order to enable areas for the RealPresence Resource Manager, login to the system with a user who has the administrator role.

Users will need to log out and log back in to the RealPresence Resource Manager in order for them to view any changes.

To enable the areas feature

1. Go to Admin > Areas.
2. From the list of Actions, select Configure Areas.
3. In the Configure Areas dialog box, ensure that the Enable Areas functions in Resource Manager box is checked.
4. Optionally, choose a name in which to refer to areas. For example, you can rename Area and Areas to Tenant and Tenants.
5. Click Save Configuration.

Create Areas for Tenants

For each new tenant, do the following:

1. Create a new area for the new tenant.
2. Give the area a name that appropriately identifies the tenant.
3. Create a user that will manage this area. You can do either of the following (or both).
   - Add at least one user to the tenant area who has the Area Administrator role and is set up to manage the area. That person can then manage their area themselves, including adding other users to manage the area and its resources.
   - You can also allow a user that belongs to no area or another area to manage the area and perform tasks, “Assign Users to Manage an Area(s)” on page 295.

Set up Area Management

The RealPresence Resource Manager allows you flexibility when setting up how to manage an area.
Manage the Area with System Roles

You can either have a set of users with system roles who manage the administrative and conference scheduling tasks for an area or you can set up area users with these roles and responsibilities.

In order for a user to perform tasks within ALL areas, a user must be given a system role that includes the View and/Or Modify all Areas permission. All system roles have this permission by default.

Manage the Area with Area Roles

In order for a user to perform tasks within a single area, a user must be given the following:

- An area role
- Be configured to manage the area to which they need to perform their tasks.

When associating a user with an area role, you must also explicitly configure that user to manage the area. If the user is not allowed to manage the area, he cannot perform the tasks associated with his role. Area users can be configured to manage more than one area, see “Assign Users to Manage an Area(s)” on page 295.

Assign Resources to an Area

You need to assign resources to an area. Resources that belong exclusively to an area must be assigned to the area. Most resources can be created and assigned to an area by an Administrator or an Area Administrator.

Network devices must be assigned to an area by someone with the Device Administrator role.

Can Belong to One or No Area

The following resources need to be assigned to one area or no area.

- Users
- Rooms
- Guests
- Groups
- Address Books
• Endpoints
• Network Devices
• Conferences
• Conference Templates
• Machine Accounts
• Peripherals

Can Belong to One or More Areas (or no Area)

Resources that can be associated with one or more areas or no areas are:
• DMA Pool Orders

Add Users to An Area

When you add users, create user names using the email address format. This will ensure that all user names are unique. Otherwise two people named Bob Smith belonging to different tenants may end up with the same user name. By following an email address format, Bob Smith in TenantA could have bsmith@tenantA.com as a user name and Bob Smith in TenantB could have bsmith@tenantB.com.

Configure Site Topology

You can use site topology to limit the bandwidth used by each tenant. This can be accomplished with a combination of a carefully organized site topology and the Site Statistics tool.

You can assign a site to a particular area. A site cannot be shared between areas.

Use the following guidelines:

• As a best practice, use a naming convention that identifies the area in the site name. For example, all sites in the blue area should be named blue_<sitename>.
• Site names should be unique across the system. That is, two areas should not use the same site name.
• At a minimum, each site in an area should have a site link to the service provider or the internet cloud. It is best practice that the purpose of each link be obvious from the site link name. Any site link being used to measure bandwidth for a specific tenant should be named in such a way as to make this purpose clear.
Endpoints and devices should be associated with the same area to which their site belongs or they may not be visible to area constrained users when searching by site.

*Figure 34-1 Site Topology for Multiple Tenants*
Managing Areas

This chapter describes how to manage areas in the Polycom® (Resource Manager™) system. It includes these topics:

- “View All Areas” on page 409
- “View Information for a Specific Area” on page 410
- “Customize the Area Logos (system and CMA Desktop) for the Area” on page 412

View All Areas

You can view the list of existing areas from Admin > Areas if you have the Administrator role. The following information is available.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the area.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the area.</td>
</tr>
<tr>
<td>Area Resource Manager Users</td>
<td>Number of users that can manage the selected area.</td>
</tr>
<tr>
<td>Endpoints</td>
<td>Number of endpoints that belong to the selected area</td>
</tr>
<tr>
<td>Rooms</td>
<td>Number of rooms that belong to the selected area.</td>
</tr>
<tr>
<td>Members</td>
<td>Number of users that belong to the selected area.</td>
</tr>
</tbody>
</table>
View Information for a Specific Area

You can view all information for a specific area including resources and users. You must be assigned the Administrator role to do this task.

To view information for a specific area

1 Go to Admin > Areas.
2 Click an area in the list.
3 The following View actions are available. The details you can view from each action is dependent on the type of resource it is. The following resources are available:
   - View Area Rooms. For more information, see “View the Rooms List” on page 356.
   - View Area Resource Manager Users. This action displays a list of all users who are allows to managed the selected area. For more information, see “View User Information” on page 278.
   - View Area Endpoints. For more information, see “View Device Details” on page 86.
   - View Area Guests. For more information, see “User Menu and Guest Book” on page 296.
   - View Area Members. This action provides a list of all users that belong to the selected area. For more information, see “View User Information” on page 278.
   - View Guests. For more information, see “Manage System Guest Book” on page 296.
   - View Area Groups. For more information, see “Manage Groups” on page 289.
   - View Area Address Books. For more information, see “Using Multiple Address Books” on page 385.
   - View Area Conference. For more information, see “Conference and Participant Management Operations” on page 53.
   - View Direct Conference Templates. For more information, see “Direct Conference Templates” on page 334.

Removing an Area

When you no longer need an area, you can either move the area’s contents to another area or delete the area and all its contents. A user must have the Administrator role in order to move or delete an area.
Consider which of these approaches is right for the area:
If you wish to delete an area and all of its resources, then:
1 Backup your data.
2 Use the Delete action to delete the area and its resources.
If you wish to delete the area, but keep all of its resources in the Resource Manager system, then:
1 Use the Move Contents action to move all of the area’s resources to another area or to no area. Move Contents will also delete the area from which contents are moved.
If you wish to keep some of the area’s resources, but delete the rest, then:
1 Edit the resources you would like to keep and reassign them to other areas or to no area.
2 Backup your data.
3 Use the Delete action to delete the area and its remaining resources.

**Moving the Contents of an Area**

If you wish to delete the area, but keep all of its resources in the Resource Manager system, then you can move the contents of the area.

When you move the contents of an area:
• All resources will now belong to the specified destination (an area or no area).
• The area and any custom logos are deleted.
• Any users who managed the moved area will not be automatically allowed to manage the new area. If you want the moved users to manage the destination area, you will need to explicitly edit the user to do so.

**Deleting an Area and its Resources**

If you no longer need an area and its resources, you can delete the area and its resources from the RealPresence Resource Manager system.

Before deleting an area, you must manually un-assign any network devices from the area. You should also verify that there are no ongoing conferences or area users involved in a conference belonging to another area.

When you delete an area, the following actions take place:
• All future conferences are cancelled.
• All past conferences are associated with no area (None).
• All pool orders are disassociated from the area.
Users, rooms and endpoints from this area that have been participants, or are invited to be participants, in other areas’ past or future conferences are disassociated from those conferences, such that:

- Resource Manager system conference reports for other areas will no longer include this area’s participants.
- Future conferences for other areas will no longer include any participant from this deleted area. If a future conference is left with only one participant as a result, the conference will be canceled and the remaining participant will be notified.

If the previous action leaves any future conference in another area with only one participant, then the conference will be cancelled and the remaining participant will be notified by email.

If a conference template belonging to this area is referenced by a conference in another area, the template will be moved to no area. Otherwise the template is deleted.

All other resources in this area are deleted.

CDR data is not deleted or modified.

---

**Disabling the Areas Feature**

Disabling areas is not yet supported.

---

**Customize the Area Logos (system and CMA Desktop) for the Area**

You can customize the logos that a RealPresence Resource Manager area user sees when they log in to the RealPresence Resource Manager system or to their CMA Desktop client.

You must have the administrator role in order to customize logos. You can only customize logos for areas that you are allowed to manage.

---

**Note**

The RealPresence Resource Manager must be running on an Internet Explorer browser in order to upload an image file.
To customize the system logo for an area
1  Go to Admin > Area Logos.
2  Click Set Resource Manager System Logo.
3  In the Set Resource Manager System Logo dialog box, browse to a file to upload and click Upload.
4  When the upload is complete, click OK.

To customize the CMA Desktop logo for CMA Desktop users within the area
1  Go to Admin > Area Logos.
2  Click Set Resource Manager System Logo.
3  In the Set Resource Manager System Logo dialog box, browse to a file to upload and click Upload.
4  When the upload is complete, click OK.
This chapter describes how to update the Polycom® Resource Manager™ system configuration settings, many of which were entered during First Time Setup. It includes these topics:

- “Edit the System Network Settings” on page 415
- “Edit the System Time Settings” on page 416
- “Integrate with Microsoft Exchange Server for Calendaring Management” on page 417
- “View Current System Licensing” on page 420
- “Add System Licenses” on page 423
- “Reclaim Polycom CMA Desktop and RealPresence Mobile Licenses” on page 424
- “Add or Remove a System Logo” on page 424
- “Add or Remove a Polycom CMA Desktop Custom Logo” on page 425
- Edit the System E-mail Account

**Edit the System Network Settings**

Edit the system Network settings to change the basic network information for the Resource Manager system.

**To edit the Resource Manager system network settings**

1. Go to Admin > Server Settings > Network.
2 Configure these settings on the **Network** page, as necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>The NetBIOS name (ASCII only) of the Resource Manager system server. Must be between 6 and 16 characters long; dashes and underscores are valid characters.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>The static IPv4 address for the Resource Manager system.</td>
</tr>
<tr>
<td>IPv4 Subnet Mask</td>
<td>The network subnet mask for the Resource Manager system IP address.</td>
</tr>
<tr>
<td>IPv4 Default Gateway</td>
<td>The static IP address of the Resource Manager system gateway.</td>
</tr>
<tr>
<td>DNS Domain</td>
<td>The DNS domain name suffix for the network in which the domain name server and Resource Manager system server reside. For example polycom.com, not the fully qualified path of &lt;hostname&gt;.polycom.com.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If instead of entering a single domain controller, you enter an FQDN that maps to multiple servers, be sure that all of the mapped servers are directory domain controllers with global catalogs.</td>
</tr>
<tr>
<td>Preferred DNS Server</td>
<td>The IP address of the preferred domain name server for the network.</td>
</tr>
<tr>
<td>Alternate DNS Server</td>
<td>The IP address of the alternate domain name server for the network.</td>
</tr>
</tbody>
</table>

3 Click **Update**.

If you change the IP address, the system prompts you to restart the Resource Manager system. We also recommend that you restart the system if you change the subnet mask.

4 As required, restart the system.

### Edit the System Time Settings

Edit the **System Time** server settings to change the Resource Manager system server time or to synchronize the server with an external NTP server.
To edit the Resource Manager system time settings

1. Go to Admin > Server Settings > System Time.
2. Configure these settings on the System Time page, as necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Time Zone</td>
<td>The time zone in which the Resource Manager system server resides.</td>
</tr>
<tr>
<td>Use Current Time</td>
<td>Select this option to input the current date and time.</td>
</tr>
<tr>
<td>Use External NTP Server Time</td>
<td>Select this option to synchronize the Resource Manager system date and time</td>
</tr>
<tr>
<td>Synchronization</td>
<td>with an external NTP server.</td>
</tr>
<tr>
<td>IP address or DNS resolved</td>
<td>The IP address or fully qualified domain name (ASCII only) of the NTP server.</td>
</tr>
<tr>
<td>name</td>
<td>If needed, enter multiple servers separated by a space.</td>
</tr>
</tbody>
</table>

**Note**

Make sure the current system time is correct before synchronizing with an NTP server. If you set the system to use an external NTP server when the current date and time are incorrect, the system time may be wrong for the amount of time specified in the **Minutes between synchronization attempts**.

3. Click Update.

Integrate with Microsoft Exchange Server for Calendaring Management

The Resource Manager system can be used to provision Polycom Conferencing for Microsoft Outlook, which is reservationless conferencing. When you use Polycom Conferencing for Microsoft Outlook:

- Video bridge, network resources, and video endpoints are not reserved at the scheduled time.
- A Polycom RMX or DMA system is required to locate available bridge resources when the meeting begins.
- Calendars for the endpoints are stored and maintained by Microsoft Exchange and the endpoints have their own Outlook calendar.

Polycom Conferencing for Outlook, which requires the Polycom Conferencing Add-in, allows:

- Conference organizers to:
— Use Microsoft Outlook and its usual meeting request workflow to schedule video- and audio-enabled meetings.
— Include recording and streaming into the conference, when required.

• Meeting participants to:
  — Track their video- and audio-enabled meetings on the same calendar that they track their other meetings.
  — Click a link in an E-mail meeting request to join conferences on their associated video or audio endpoint system.

• Endpoints to have their own unique credentials and mailbox separate from the endpoint user, so that endpoints can display their own calendars. This is especially important for room endpoints.

To provision endpoints with the information required to support Polycom Conferencing for Outlook, you must complete the following tasks (after your sites are set up):

1 “Associate Sites with Microsoft Exchange Servers” on page 418.
2 “Assign Calendaring Settings to Provisioning Profiles” on page 419.
3 “Provision the Exchange Mailbox for Calendaring Service-enabled Endpoints” on page 419.

## Associate Sites with Microsoft Exchange Servers

By default, the Resource Manager system is set up to automatically discover the Exchange server for the domain in which a site is located. However, if you wish to associate sites with an Exchange server using its IP address or DNS name, follow this procedure.

**To associate sites with Microsoft Exchange servers by IP address or DNS name**

1 Go to Admin > Server Settings > Calendaring Management.
2 In the Manage Calendaring dialog box, click Calendared Sites.
   The Specify Calendaring Exchange Servers page appears listing the sites defined on the Resource Manager system.
   When areas are enabled on your system, this field shows a value of Restricted if you do not have permission to manage the area to which the site is assigned.
3 Select the check box for each of the sites you need to associate with a single Exchange server and then click Specify Exchange Server.
4 In the Add Exchange Server dialog box, enter the Exchange Server Address or DNS and click Save.
   The sites appear in the calendared sites list below.
5 Repeat steps 3 and 4 for each Exchange server for which you need to associate sites.

Assign Calendar Settings to Provisioning Profiles

Calendar settings are included as part of provisioning profiles.

**To assign calendar settings to provisioning profiles**

1. Go to Admin > Server Settings > Calendaring Management.
2. In the Manage Calendaring dialog box, click Group Information.
   The Group Information page appears listing the provisioning profiles defined on the Resource Manager system.
3. Select the check box for each of the provisioning profiles to which you need to assign the same calendaring settings and then click Specify Options.
4. In the Manage Calendaring dialog box, configure these options.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting Reminder Time</td>
<td>Specifies the number of minutes before the meeting an endpoint system provisioned for Polycom Conferencing for Outlook will display a reminder.</td>
</tr>
<tr>
<td>Enable Alert Tone</td>
<td>When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will play a sound along with the meeting reminder. In this case, the endpoint will only play a sound when the system is not in a call.</td>
</tr>
<tr>
<td>Display Private Meetings</td>
<td>When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will display details about meetings marked private.</td>
</tr>
</tbody>
</table>

5. Click Save.
   The profiles appear in the calendared profiles list below.

6. Repeat steps 3 through 5 for each set of profiles to which you need to assign calendaring settings.

Provision the Exchange Mailbox for Calendaring Service-enabled Endpoints

To use Polycom Conferencing for Outlook (PCO), a Polycom endpoint system must have a mailbox on the assigned Exchange server, and the Exchange server must authenticate the endpoint before it can access its mailbox.
To use the Resource Manager system to automatically provision a Polycom endpoint system, the endpoint system must use the same credentials (username and password) to access both the Exchange server and the Resource Manager system. Only then can the Resource Manager system automatically provision a calendaring service-enabled endpoint system.

To provision the Exchange Mailbox for calendaring service-enabled endpoints

1. Go to Admin > Server Settings > Calendaring Management.
2. In the Manage Calendaring dialog box, click Mailbox.
3. In the Polycom Conferencing for Outlook page, enable Provision Mailbox and click OK.

For Exchange credentials, each endpoint system will be provisioned with the same credentials it used to access the Resource Manager system.

For its mailbox, each endpoint system will be provisioned with the mailbox configured for it in Active Directory. This mailbox must be pre-configured for the endpoint system on the Exchange server.

View Current System Licensing

To view current Resource Manager system licensing

➢ Go to Admin > Server Settings > Licenses.

The Licenses page displays the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Version</td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td></td>
</tr>
<tr>
<td>Supported Versions</td>
<td></td>
</tr>
<tr>
<td>Server Type</td>
<td></td>
</tr>
<tr>
<td>License Status</td>
<td></td>
</tr>
</tbody>
</table>

System Licensing

The device management capacity for a RealPresence Resource Manager system with the scales from 500 to 10,000 devices. The minimum capacity of a RealPresence Resource Manager system is of 500 client access licenses. Additional licensing is offered in 100, 500, and 1000 license pack sizes.
Your system comes with a Default Trial license file that is valid for 60 days after activating your system. The Default Trial License also enables the optional Polycom DMA system integration, multi-tenancy, and Service Provider API capabilities for 60 days.

With your system order, you will receive one License Certificate. You must activate the License Certificate to receive a license file, which you then upload to the Resource Manager system. When you update this license file, it overwrites the Default License File.

When applied to the system, an expansion license pack augments the device license count. For example, applying a 1000-device expansion license pack to a baseline Resource Manager system will yield a total license count of 1500 concurrent licenses.

Device licenses are consumed based on a 1:1 basis for any managed device (endpoints, MCU, GW — including personal endpoints, IP blades, and more) that can be added to the system by any means, including the user interface, registration for management services, or registration for Global Address Book services.

**Note**

Device licenses are consumed by managed devices, not by users. You may add any number of local or enterprise users to the Resource Manager system.

The Resource Manager system has the following feature licenses:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMA Integration</td>
<td>Allows you to integrate with a Polycom DMA system as both a call server (gatekeeper) and conference manager</td>
</tr>
<tr>
<td>Multi-Tenant</td>
<td>Allows you to use the areas feature to partition collections of resources.</td>
</tr>
<tr>
<td>Management of Endpoints and Services</td>
<td>Determines the number of devices you can manage.</td>
</tr>
<tr>
<td>Service Provider API</td>
<td>Allows you to access RealPresence Resource Manager functionality via the API</td>
</tr>
<tr>
<td>Redundant system licenses (primary and redundant licenses)</td>
<td>Allows you to set up redundant systems.</td>
</tr>
</tbody>
</table>

Licensing for RealPresence software clients is included with the Resource Manager system. RealPresence software clients include Polycom CMA Desktop and RealPresence Mobile clients.
When either client is provisioned by the Resource Manager system, it automatically consumes a license. That license is then reserved for that client. However, you can configure the system to automatically release a RealPresence client license after a set number of days of inactivity.

Licenses consumed by registered hardware devices are never automatically released. To release a license from a registered hardware device, an administrator must manually delete the device from the system.
Add System Licenses

Adding licenses to your Resource Manager system is a two step process:

- “Request a Software License File” on page 423.
- “Update the License File” on page 423

These processes are described in the following topics.

Request a Software License File

To request a software license file

1. In a separate browser page or tab, log into the Resource Manager system server as an administrator.

2. Go to Admin > Server Settings > Licenses and record the Resource Manager system server serial number:


4. In the Licensing & Product Registration section, select Activation/Upgrade.

5. Log in or Register for an Account.


7. In the Site & Single Activation page, enter the serial number you recorded in step 2.

8. Click Next.

9. Accept the EXPORT RESTRICTION agreement.

10. In the new Site & Single Activation page, enter the serial number listed on your License Certificate and enter the license number (shipped with the product) and click Activate.

   If retrieving licenses for a redundant system, repeat this step for each server in your configuration. You will need to load both license files onto your primary server, see “System Redundancy” on page 439.

11. In the Key Code field, click click here to download to retrieve and save your license files.
Update the License File

To update the license file
1. Go to Admin > Server Settings > Licenses.
2. Click Update License to view the Update License dialog box.
3. Click Choose File to navigate to the license file you received from Polycom.
4. Click Preview to preview the license features.
5. On the Update License dialog box, click Update.

Reclaim Polycom CMA Desktop and RealPresence Mobile Licenses

Neither the Polycom CMA Desktop or the RealPresence Mobile client release licenses automatically when they are not in use. You can reclaim software client licenses by setting a reclaim threshold.

To reclaim licenses more quickly, lower the threshold. Set the threshold to zero, to stop reclaiming licenses.

To set the threshold for reclaiming inactive RealPresence Software Client licenses
1. Go to Admin > Server Settings > Licenses.
2. Change the Threshold value in the Reclaim Inactive RealPresence Software Client (Mobile and Desktop) Licenses section of the Licenses page. To reclaim licenses more quickly, lower the threshold. Set the threshold to zero, to stop reclaiming licenses.
3. Click Update.
Add or Remove a System Logo

You can add your company’s logo to the Resource Manager system user interface. To avoid distortion, we recommend adding a logo in GIF, JPG, or PNG format with a size of 300 x 44 pixels.

**When Areas Are Enabled**
- The system logo added with these steps is viewed only by users with system roles that have permission to view all areas and do not belong to an area.
- To customize a logo for an area, you must use the Admin > Area Logos option, see Customize the Area Logos (system and CMA Desktop) for the Area.

**To add a custom logo to the Resource Manager system user interface**
1. Go to Admin > Server Settings > System Logos.
2. In the Current Logo section of the System Logos page, click Upload...
3. In the Select file dialog box, browse to the logo image and select the file.
4. Click Open.
5. In a redundant configuration, repeat steps 1 through 4 on the redundant server.

**To remove a system logo from the Resource Manager system user interface**
1. Go to Admin > Server Settings > System Logos.
2. In the Current Server Logo section of the System Logos page, click Remove.
Add or Remove a Polycom CMA Desktop Custom Logo

You can add your company logo to the Polycom CMA Desktop user interface. This logo will be displayed on the application user interface before the user logs in. The following illustration shows the default Polycom CMA Desktop user interface and a customized Polycom CMA Desktop user interface.

To avoid distortion, use a logo in GIF or JPG format with a size of approximately 260x215 pixels.

Because the Polycom CMA Desktop logo is stored in the Resource Manager system database, in redundant configurations you do not need to upload the logo to both servers.

To add a custom logo to the CMA Desktop user interface

1. Go to Admin > Server Settings > System Logos.
2. In the CMA Desktop Logo section of the System Logos page, click ... to browse to a logo file to use.
3. In the Select file dialog box, browse to the logo image and select the file.
4. Click Open.
5. Click Upload.

Once a user logs in, is provisioned, and then logs out, the logo will be displayed on the Polycom CMA Desktop user interface.

To remove a custom logo from the CMA Desktop user interface

1. Go to Admin > Server Settings > System Logos.
In the Current CMA Desktop Logo section of the System Logos page, click Restore Default. Once a user logs in, is provisioned, and then logs out, the default logo will be displayed on the CMA Desktop user interface.

**Edit the System E-mail Account**

**To edit the Resource Manager system e-mail account**

1. Go to Admin > Server Settings > E-mail.
2. On the E-mail page, edit the e-mail account (ASCII only) from which the Resource Manager system will send conference notification e-mails or edit the IP address of the mail server from which the Resource Manager system will send conference notification e-mails.

**Notes**

- Many e-mail servers will block or discard e-mails without a qualified From: address. To avoid this issue, make sure each person with Scheduler permissions has a valid E-mail address.
- Many E-mail servers will block or discard e-mails from un-trusted domains, in which case you may need to change the default Resource Manager system E-mail address to one in a trusted domain.

3. Click Update.
This chapter provides a discussion of the Polycom® RealPresence® Resource Manager system SNMP support. It includes these topics:

These topics provide a discussion of the Polycom® RealPresence® Resource Manager system SNMP support. They include:

- “SNMP Overview” on page 427
- “Working with SNMP” on page 429

**SNMP Overview**

Simple Network Management Protocol (SNMP) is a TCP/IP-based communication protocol that allows network management systems to manage resources across a network.

SNMP communication takes place between the management system and SNMP agents, which are the hardware and software that the management system monitors. An agent collects and stores local system information and makes this information available to the management system via SNMP.

The RealPresence Resource Manager system includes an SNMP agent. It translates local system information into the format defined by the MIB.

The RealPresence Resource Manager system resides on a Polycom-branded Dell server. The Dell server software also includes an SNMP agent and MIB (Message Information Base). However, the RealPresence Resource Manager system acts as a proxy agent to forward the Dell server MIB alarms and alerts, so the management system does not need to be configured to receive information directly from the Dell server MIB.
Polycom recommends using a MIB browser to explore the RealPresence Resource Manager system MIB. However, a printed copy of the MIB is available in “MIB Reference” on page 527. The RealPresence Resource Manager system MIB is self-documenting and includes information about the purpose of specific traps and inform notifications.

It is important to note that you should understand how your SNMP management system is configured to properly configure the RealPresence Resource Manager system SNMP transport protocol requirements, SNMP version requirements, SNMP authentication requirements, and SNMP privacy requirements on the RealPresence Resource Manager system.

The RealPresence Resource Manager system supports three SNMP levels:

- **Disabled** – The RealPresence Resource Manager system SNMP processes are turned off.

- **SNMPv2c** – The RealPresence Resource Manager system implements a sub-version of SNMPv2. The key advantage of SNMPv2c is the Inform command. Unlike Traps, Informs are messages sent to the management system that must be positively acknowledged with a response message. If the management system does not reply to an Inform, the RealPresence Resource Manager system resends the Inform. SNMPv2c also has improved error handling and improved SET commands.

  One drawback of SNMPv2c is that it is subject to packet sniffing of the clear text community string from the network traffic, because it does not encrypt communications between the management system and SNMP agents.

- **SNMPv3** – The RealPresence Resource Manager system implements the newest version of SNMP. Its primary feature is enhanced security. The contextEngineID in SNMPv3 uniquely identifies each SNMP entity. The contextEngineID is used to generate the key for authenticated messages.

  The RealPresence Resource Manager system implements SNMPv3 communication with authentication and privacy (the authPriv security level as defined in the USM MIB).

  - Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the contextEngineID of the entity. The key is shared with the intended recipient and used to receive the message.

  - Privacy encrypts the SNMP message to ensure that it cannot be read by unauthorized users.
Working with SNMP

This section describes the system SNMP operations including:

- “Enable SNMP Messaging” on page 429
- “Edit the SNMP Settings for a RealPresence Resource Manager System” on page 429
- “Add an SNMP Notification Receiver” on page 431
- “Download RealPresence Resource Manager System MIB Package” on page 433

Enable SNMP Messaging

To enable SNMP messaging you must perform the two tasks:

1. “Edit the SNMP Settings for a RealPresence Resource Manager System” on page 429
2. “Add an SNMP Notification Receiver” on page 431

Edit the SNMP Settings for a RealPresence Resource Manager System

To edit the SNMP settings for a RealPresence Resource Manager system

1. Go to Admin > SNMP Settings.
2. To enable SNMP, select an SNMP Version. For information on the SNMP versions, see “SNMP Overview” on page 427.
3. Configure these settings for the connection between the RealPresence Resource Manager system and the SNMP agents on the SNMP Setting page.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocols:</td>
</tr>
<tr>
<td></td>
<td><strong>TCP</strong>—This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent. Some SNMP managers only support SNMP over TCP.</td>
</tr>
<tr>
<td></td>
<td><strong>UDP</strong>—This protocol does not provide error-recovery services, message delivery is not assured, and messages are not necessarily delivered in the order they were sent. Because UDP doesn't have error recovery services, it requires fewer network resources. It is well suited for repetitive, low-priority functions like alarm monitoring.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port that the RealPresence Resource Manager system uses for general SNMP messages. By default, the RealPresence Resource Manager system uses port 161.</td>
</tr>
<tr>
<td>Community</td>
<td>For SNMPv2c, specifies the context for the information, which is the SNMP group to which the devices and management stations running SNMP belong.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence Resource Manager system has only one valid context—by default, public—which is identified by this <strong>Community</strong> name. The RealPresence Resource Manager system will not respond to requests from management systems that do not belong to its community.</td>
</tr>
<tr>
<td>V3 Context Name</td>
<td>For SNMPv3, specifies the context for the information. The RealPresence Resource Manager system has only one valid context, which is identified by contextName (in our case—an empty string) and contextEngineId.</td>
</tr>
<tr>
<td>V3 Local Engine Id</td>
<td>For SNMPv3, displays the RealPresence Resource Manager system contextEngineId for SNMPv3.</td>
</tr>
<tr>
<td>Security User</td>
<td>For SNMPv3, specifies the security name required to access a monitored MIB object.</td>
</tr>
</tbody>
</table>
Add an SNMP Notification Receiver

You can configure the RealPresence Resource Manager system to send SNMP messages to different notification receivers (e.g., a network management system).

To add an SNMP notification receiver to the system
1. Go to Admin > SNMP Settings.
2. In the Notification RCVR Actions section, click Add.
3 Configure these settings in the **New Notification Receiver** dialog box.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Specifies the IP address of the host receiver.</td>
</tr>
</tbody>
</table>
| Transport          | Specifies the transport protocol for SNMP communications to the host receiver. Possible values are:  
|                    | • TCP                                                                       |
|                    | • UDP                                                                       |
| Port               | Specifies the port that the RealPresence Resource Manager system will use to send notifications. By default, the RealPresence Resource Manager system uses port 162. |
| Trap/Inform        | Specifies the type of information that should be sent to the host receiver. Possible values are:  
|                    | • Inform—An unsolicited message sent to a notification receiver that expects/requires a confirmation message. Introduced with SNMP version 2c, this option is not supported by systems that only support SNMP version 1.  
|                    | • Trap—An unsolicited message sent to a notification receiver that does not expect/require a confirmation message. |
| SNMP Version       | For SNMPv3, specifies the context for the information.  
|                    | The RealPresence Resource Manager system is a proxy-forwarding application. It passes SNMP requests to its various SNMP-reporting processes based on the context information in the SNMP message. For SNMPv3, this context is identified by contextName and contextEngineID. |
| V3 Local Engine Id | For SNMPv3, displays the RealPresence Resource Manager system contextEngineID for SNMPv3. |
| Security User      | For SNMPv3, specifies the security name required to access a monitored MIB object. |
Download RealPresence Resource Manager System MIB Package

To download the MIB package for a RealPresence Resource Manager system

1  Go to Admin > SNMP Settings.
2  Click Download Resource Manager MIBs.
3  In the Resource Manager MIBs dialog box, select the MIB of interest.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auth Type        | For SNMPv3, specifies the authentication protocol. The RealPresence Resource Manager system implements communication with authentication and privacy (the authPriv security level as defined in the USM MIB). Possible values for authentication protocol are:  
  • MD5  
  • SHA  
  These protocols are used to create unique fixed-sized message digests of a variable length message. MD5 creates a digest of 128 bits (16 bytes) and SHA creates a digest of 160 bits (20 bytes). |
| Auth Password    | For SNMPv3, specifies the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest. |
| Encryption Type  | For SNMPv3, specifies the privacy protocol for the connection between the RealPresence Resource Manager system and the notification receiver. The RealPresence Resource Manager system implements communication with authentication and privacy (the authPriv security level as defined in the USM MIB). Possible values for privacy protocol are:  
  • DES  
  • AES  |
<p>| Encryption Password | For SNMPv3, specifies the password to be associated with the privacy protocol. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adptInfo-MIB</td>
<td>The interface table (ifTable) shows addresses, physical addresses, names, descriptions etc. of the network interfaces</td>
</tr>
<tr>
<td>baspcfg</td>
<td>The interface table (ifTable) shows addresses, physical addresses, names, descriptions etc. of the network interfaces</td>
</tr>
<tr>
<td>baspStat</td>
<td></td>
</tr>
<tr>
<td>baspTrap</td>
<td></td>
</tr>
<tr>
<td>DcAsfSrv</td>
<td>Trap definitions for the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.</td>
</tr>
<tr>
<td>dcs3fru</td>
<td>Contains all the field replaceable unit names, serial numbers, and revisions for the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.</td>
</tr>
<tr>
<td>DcAsfSrv</td>
<td>Trap definitions for the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.</td>
</tr>
<tr>
<td>dcs3rmt</td>
<td>Provides information about server administrator remote access.</td>
</tr>
<tr>
<td>INET-ADDRESS-MIB</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>INTELLAN</td>
<td>Information about the Intel LAN.</td>
</tr>
<tr>
<td>ITU-ALARMS-TC-MIB</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>10892</td>
<td>The primary MIB for the Polycom-branded Dell server. It provides 36 traps from the server motherboard, including system type, voltages, and temperature readings. For more information, see the Dell SNMP documentation.</td>
</tr>
<tr>
<td>ITassist</td>
<td>IT assistant.</td>
</tr>
<tr>
<td>Dell-RAC-MIB</td>
<td>Information about the Dell Remote Access Controller.</td>
</tr>
<tr>
<td>POLYCOM-RM-MIB</td>
<td>Resource Manager-specific MIB definition</td>
</tr>
<tr>
<td>RFC1213-MIB</td>
<td>RFC1213MIB definitions included for reference. The RealPresence Resource Manager system supports all but &quot;egp&quot;.</td>
</tr>
<tr>
<td>SNMPv2-CONF</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
</tbody>
</table>
Polycom recommends using a MIB browser to explore the RealPresence Resource Manager system MIB. However, a printed copy of the MIB is available in “MIB Reference” on page 527. The RealPresence Resource Manager system MIB is self-documenting including information about the purpose of specific traps and inform notifications.

### Change the SNMP Communication Port

By default, the RealPresence Resource Manager system uses port 161 as its standard open port for SNMP communications. However, you can change this to another open port.

**To change the SNMP communication port**

1. Go to Admin > SNMP Settings.

2. In the Port field of the SNMP Settings page, type a new communication port number and click Update SNMP Settings.
Managing the Database

This chapter describes the Polycom® RealPresence® Resource Manager database integration and operations. It includes these topics:

- “Overview of the RealPresence Resource Manager System Database” on page 437
- “Database Restoration” on page 437
- “Reformat the Existing Database” on page 438

Overview of the RealPresence Resource Manager System Database

The RealPresence Resource Manager system automatically optimizes its internal database on an ongoing basis. Database backup files are created when you run system backups, see “Backup the System Settings” on page 515.

Database Restoration

You can restore the database by performing a system restoration, see “Restore from a Backup Archive” on page 517.
Reformat the Existing Database

The RealPresence Resource Manager system has an option that allows you to completely reformat (clean out) the system’s existing database.

Use this option only if your database is corrupted beyond repair or perhaps if you need to wipe out a test system to prepare it for production data.

To reformat the existing database

1. From the RealPresence Resource Manager system web interface, go to **Admin > Server Settings > Database**.

2. On the **Database** page, select **Reformat existing database...**

3. Click **Yes** to confirm the reformat operation.

   The system displays a **Reformat/Install Progress** bar to indicate that the system is reformattting the database.
This chapter describes how to configure a redundant Polycom® Resource Manager™ system.

It includes these topics:

- “System Redundancy Overview” on page 439
- “Implement a Redundant System” on page 442
- “Failover to a Redundant Server” on page 444
- “Discontinue Redundancy” on page 444

**System Redundancy Overview**

A redundant Resource Manager system configuration offers higher reliability and greater call success by ensuring that a Resource Manager system server is always available.

A redundant Resource Manager system configuration requires two Resource Manager system servers and three IP addresses in the same subnet on the same network—one physical IP address for each of the servers and one virtual IP address dedicated to external access and endpoint registration.

This section includes the following topics:

- “How Redundancy Works” on page 440
- “Redundant Configuration System Administration” on page 441
- “Considerations for Redundancy” on page 441
How Redundancy Works

Terminology is very important in understanding how redundancy works. In a redundant configuration, one server is licensed as the primary server and the other server is licensed as the redundant server. The primary server is always the primary server and the redundant server is always the redundant server.

In a redundant configuration, there is only one active server and only one inactive server. The active server is the server managing the system. It is the server running all of the Resource Manager system services. In a normal operational state, the active server is the primary server. In a failover state, the active server is the redundant server.

The active/inactive servers communicate every 200 milliseconds using a private IP address and port 5405. If the inactive server does not receive a heartbeat from the active server, it will promote itself to being the active server.

The most common reasons for system failovers are power failures and network disconnections. Failures in services also initiate a failover.

If both the primary and redundant servers start simultaneously (for example if both are in the same location and recover from a power failure at the same time), both servers will initially attempt to become the active server. Whichever server starts first becomes the active server.

An administrator can force a failover via the Switch Server Role function in the Resource Manager system user interface.

Also, the failover to the redundant server seems to occur seamlessly because the endpoints are registered with the virtual IP address, which remains constant. However, endpoints that are dynamically managed will lose the connection as the provisioning service will stop for approximately five minutes.

During a failover:

- Users logged into the Resource Manager system user interface are disconnected during a failover and returned to the main Resource Manager system web page. Users can log back in once the failover is completed.
- Users in the middle of an operation may get an error message, because the system is not available to respond to a request.
- The redundant server becomes the active server. Its services start in an order designed to prevent the new active server from being flooded with requests from endpoints during startup.

A system failover usually takes approximately 5 minutes.

Once a failover to a redundant server occurs, the redundant server manages all system operations until an administrator switches back to the original primary server via the Switch Server Roles function in the Resource Manager system user interface.
Redundant Configuration System Administration

The system database is replicated between the two servers so most of their configuration information is shared. However, certain information is not stored in the database, so an administrator must manually synchronize this information.

The following settings must match between the two servers and be configured before setting up redundancy.

This includes:

• Basic network settings such as IP, default gateway, and DNS settings
• Time and external NTP server settings

Whenever you change information in one of these sections on one server you should also change it on the other server.

Licensing

Licensing and upgrading a redundant system is slightly more complex. The primary and redundant server require different licenses.

Data Loss

Under some circumstances, data loss cannot be avoided. If one server has been down for quite some time, its data may be out of date. If the system fails over while out of sync, database data may be lost. This is an extreme circumstance caused by factitiously sequential faults.

Considerations for Redundancy

Consider the following:

1. During first-time set up for each server, use the same NTP server for both servers. You cannot modify the NTP server settings after setting up redundancy.
2 Ensure each system uses the same RealPresence Resource Manager software version.
3 Do NOT upload license files until you have set up redundancy.
4 Ensure both systems are up and running before configuring redundancy.
5 If configuring redundancy on an existing system, Polycom recommends making a system backup before configuring redundancy.
6 You cannot change the system name or domain name after configuring redundancy.

### Implement a Redundant System

A redundant system configuration requires the installation of two RealPresence Resource Manager system servers on the same network. During **First Time Setup**, you are instructed to assign these two servers physical IP addresses.

This section describes how to complete the configuration of these newly installed redundant servers. It includes these topics:

- “Perform a System Backup” on page 442
- “Perform Network Configuration on Both Servers” on page 442
- “Connect the Servers to Each other Via Cable” on page 443
- “Ensure You Have Appropriate Licenses for Both Servers” on page 443
- “Configure the Both Servers for Redundancy” on page 443
- “License a Redundant System” on page 443

### Perform a System Backup

If you are setting up redundancy for an existing RealPresence Resource Manager that has already been active, you should first backup your existing system. See “Backup the System Settings” on page 515.

### Perform Network Configuration on Both Servers

Install the both of your RealPresence Resource Manager systems as described in the Polycom Resource Manager Getting Started Guide.

Be sure they are both configured to the same NTP server.

Do NOT change the Factory default password until after configuring redundancy.

If setting up redundancy for an existing installation, reset the password to the factory default.
Connect the Servers to Each other Via Cable

Directly connect the servers to each other using an Ethernet or crossover cable. Place the connecting cable on the second network card.

Ensure You Have Appropriate Licenses for Both Servers

Follow the steps on “Request a Software License File” on page 423

Configure the Both Servers for Redundancy

You need to configure both servers for redundancy.

To set up redundancy for your environment

1. On the server, go to Admin > Server Settings > Redundant Configuration.
2. Enter the IP Settings for the redundant system and click Submit.

<table>
<thead>
<tr>
<th>IP Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP</td>
<td>This virtual IP address of the redundant server. You only need to configure a value for the Virtual IP address on the primary server where the primary license will be installed.</td>
</tr>
<tr>
<td>Virtual Host Name</td>
<td>The hostname that corresponds to the virtual IP address.</td>
</tr>
<tr>
<td>Local Server IP</td>
<td>This is the IP address of the local server. It is read automatically and is readonly.</td>
</tr>
<tr>
<td>Peer Server IP</td>
<td>The IP address of the second server in your configuration.</td>
</tr>
</tbody>
</table>

The primary system will reboot.

3. Verify that you can access the primary server.
4. Repeat these steps on the redundant (second) server.

License a Redundant System

This topic describes how to license a redundant system. You will need a primary license for one server and a secondary license for the second server.

To license a non-redundant Resource Manager system, see “Add System Licenses” on page 423.
To license a redundant system

1 Request a both a primary license for the primary server and a secondary license for the secondary server as described in “Request a Software License File” on page 423.

2 Log into the Resource Manager system using the virtual IP address, and go to Admin > Server Settings > Licenses.

3 Click Update License.

4 Follow the instructions on the Update License dialog and be sure you have a backup copy of your initial license file.

5 Click Choose File and navigate to the primary license file you requested.

6 Click Preview and then click Apply.

7 Click Update License again.

8 Follow the instructions on the Update License dialog

9 Click Choose File and navigate to the secondary license file you requested. Then click Apply after Preview correctly.

Failover to a Redundant Server

In a redundant configuration, the system automatically fails over from the primary server to the redundant server. However, you can also manually initiate a failover.

The Switch Server Role option is not available if the inactive server is not available.

To manually initiate a failover

1 On either server, go to Admin > Server Settings > Redundant Configuration.

2 On the Redundant Configuration page, click Switch Server Role.

   The system initiates a failover to the other server.

Discontinue Redundancy

In some circumstances, you may need to discontinue redundancy.
To discontinue a redundant Polycom Resource Manager system configuration when the system is in a valid redundant state:

Use this procedure to discontinue redundancy, but only when the system is in a valid redundant state.

1  Log into the Resource Manager system using the virtual IP address.
2  Go to Admin > Server Settings > Redundant Configuration.
3  On the Redundant Configuration page, click Reset Redundant Configuration.

The two servers restart as single server.

To discontinue a redundant Polycom Resource Manager system configuration if only one server can be accessed:

If only one server can be accessed, discontinue redundancy on that server first. Discontinue redundancy on the other server after it can be accessed

1  Log into the Resource Manager system using the virtual IP address.
2  Go to Admin > Server Settings > Redundant Configuration.
3  On the Redundant Configuration page, click Reset Redundant Configuration.

The primary system restarts as single server.

4  When the redundancy server can be accessed (Now it promotes to active server), log into the system using the virtual IP address.
5  Go to Admin > Server Settings > Redundant Configuration.
6  On the Redundant Configuration page, click Reset Redundant Configuration.

The system restarts as single server.
Securing the System

This chapter describes the Polycom® RealPresence® Resource Manager system management and security tasks. It includes these topics:

- “Update the System Software” on page 447
- “Manage Certificates” on page 448
- “Change the System User Interface Timeout and Number of Sessions” on page 456
- “Give Enterprise Users Default Scheduler Role” on page 457
- “Change the Message for Enterprise Users without a Role” on page 457
- “Control Remote Connections to the System” on page 458
- “Automatic Registration Synchronization” on page 459
- “Set Common Passwords for Endpoints” on page 460
- “Disable Common Password for Endpoints” on page 460
- “Set Local Account Lockout and Timeout” on page 461
- “Set Local Password Requirements” on page 461
- “Add Machine Accounts” on page 462
- Change Database Passwords

Update the System Software

To update a RealPresence Resource Manager system with a new software version, complete the following tasks:

1. Download the software upgrade file.
2. Obtain an upgrade key code.
3. Save a backup of the RealPresence Resource Manager system databases.

Browse to select the software upgrade file you downloaded.
5 Click Upgrade.
   A warning dialog box displays warning you NOT to close the browser.
   DO NOT log out of the RealPresence Resource Manager or close the
   browser during the upgrade. Doing so will cancel the upgrade process.

6 When the upgrade files are completely unpacked and the warning, the
   warning dialog box disappears. You can now logoff or close the browser
   window. The upgrade process continues.
   At any time during the upgrade, navigate to the following URL to view
   status:
   
   http://<REALPRESENCERESOURCEMANAGER_IP>:8989/upgrading.html

7 Verify the upgrade.

For more information on performing each of these tasks, see the Polycom
RealPresence Resource Manager System Upgrade Guide.

Manage Certificates

Certificates are a security technology that assists networked computers in
determining whether to trust each other. Each digital certificate is identified by
its public key. The collection of all public keys used in an enterprise to
determine trust is known as a Public Key Infrastructure (PKI).

To manage digital certificates, an enterprise must:

• Establish a Public Key Infrastructure using one or more Certificate
  Authorities (CA). Typically, an enterprise’s IT department has a CA but
  commercial CAs may be used as well.

• Configure each computer that participates in the PKI with a digital
  certificate that identifies it. The certificate must be signed by one of the
  CAs in the PKI

• Configure each computer that participates in the PKI to trust the PKI’s
  Certificate Authorities

• Ensure that the PKI is used to protect data exchange by configuring each
  system to use encryption protocols such as Secure Sockets Layer (SSL)
  and/or Transport Level Security (TLS).

Certificates Accepted by the RealPresence Resource Manager System

By default, to support encrypted communications and establish a minimum
level of trust, the RealPresence Resource Manager system presents a
self-signed digital certificate to its clients. This default certificate will typically
not be trusted by clients. Web browsers that connect to the RealPresence
Resource Manager system user interface will display a warning regarding the
certificate.
Participation in a Public Key Infrastructure requires a RealPresence Resource Manager system to have been configured with at least one root CA certificate, a current certificate revocation list (CRL) from the CA, and a digital certificate signed by the CA that identifies the RealPresence Resource Manager system.

Certificates come in several forms (encoding and protocol). The following table shows the forms that can be installed in the RealPresence Resource Manager system.

<table>
<thead>
<tr>
<th>Encoding</th>
<th>Standard / File Type</th>
<th>Description and Installation Method</th>
</tr>
</thead>
</table>
| PEM (Base64-encoded ASCII text) | PKCS #7 standard P7B file | Certificate chain containing:  
  • A signed certificate for the system, authenticating its public key.  
  • The CA's public certificate.  
  • Sometimes intermediate certificates.  
  Upload file or paste into text box. |
| CER (single certificate) file | PKCS #12 standard PFX file | Certificate chain containing:  
  • A signed certificate for the system, authenticating its public key.  
  • A private key for the system.  
  • The CA's public certificate.  
  • Sometimes intermediate certificates.  
  Upload file. |
| Certificate text             | PKCS #7 standard P7B file | Certificate chain containing:  
  • A signed certificate for the system, authenticating its public key.  
  • The CA's public certificate.  
  • Sometimes intermediate certificates.  
  Upload file. |
| CER (single certificate) file (X.509 standard format) | Certificate text copied from CA's E-mail or secure web page. Paste into text box. | |

Polycom, Inc.
Certificate Operations

You can set up certificates at any time.

Use the Certificate Management page to:

- View Certificates and Certificate Details
- Create a Certificate Signing Request
- Install a Certificate
- Upload a Certificate Revocation List
- Delete a Certificate

View Certificates and Certificate Details

To view the list of installed certificates

1 Go to Admin > Management and Security > Certificate Management.

The Certificate Management page displays the list of currently installed certificates. By default, the system will display only one certificate. It will be identified as the Resource Manager self-signed certificate. When other certificates are installed, they will display along with the server identity certificate.

The Certificate Management page has this information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the certificate. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Certificate is valid</td>
</tr>
<tr>
<td></td>
<td>• Certificate is invalid</td>
</tr>
<tr>
<td>Identifier</td>
<td>The certificate name as assigned by the CA</td>
</tr>
</tbody>
</table>
To view more information about a certificate, select the certificate and click View Certificate Details.

The Certificate Details dialog box appears with this information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>The type of certificate. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• RealPresence Resource Manager self-signed—the system identity certificate.</td>
</tr>
<tr>
<td></td>
<td>• Trusted root certificate—the root certificate for a CA.</td>
</tr>
<tr>
<td></td>
<td>• Intermediate certificate—certificate from an intermediate CA.</td>
</tr>
<tr>
<td></td>
<td>• Trusted peer—certificate from any server or computer that is not a CA but whose identity is</td>
</tr>
<tr>
<td></td>
<td>trusted. The trusted peer certificate must be signed by one of the CAs installed in the</td>
</tr>
<tr>
<td></td>
<td>RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Expiration</td>
<td>The expiration date of the certificate.</td>
</tr>
<tr>
<td>CRL Next Update</td>
<td>The date by which a new certificate revocation list from the CA must be uploaded.</td>
</tr>
</tbody>
</table>

**IMPORTANT**

If an administrator does not upload a new CRL by the CRL Next Update date, the system will become unresponsive. Recovering from this situation requires reinstalling from the recovery disk, manually reconfiguring of identity and root certificates, and restoring the system from a system backup.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Info</td>
<td>Purpose and alias of the certificate.</td>
</tr>
<tr>
<td>Issued To</td>
<td>Information about the entity to which the certificate was issued and the certificate serial number.</td>
</tr>
<tr>
<td>Issued By</td>
<td>Information about the issuer.</td>
</tr>
<tr>
<td>Validity</td>
<td>Issue and expiration dates.</td>
</tr>
</tbody>
</table>
Use the arrows to reveal or hide information. Click **Close** when you are done.

## Create a Certificate Signing Request

Although the initial RealPresence Resource Manager system configuration permits using the default, self-signed certificate, normal operation in a secure mode requires that you install a digital certificate signed by a trusted certificate authority that uniquely identifies the RealPresence Resource Manager system within your public key infrastructure. This can be done by creating a certificate signing request for the RealPresence Resource Manager system and submitting it to a certificate authority to be signed.

This procedure describes how to create a certificate signing request (CSR) to submit to a certificate authority.

### To create a certificate signing request

1. Go to **Admin > Management and Security > Certificate Management**.

   The **Certificate Management** page displays the list of currently available certificates. By default, the system will have one server certificate identified as the **Resource Manager self-signed certificate** and one or more root certificates or certificate chains.

2. Click **Create Certificate Signing Request**.

   If you see the warning “This action will overwrite any previously generated or uploaded private key. Do you want to continue?,” do one of the following:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprints</td>
<td>SHA1 and MD5 fingerprints (checksums) for confirming certificate.</td>
</tr>
<tr>
<td>Public Key</td>
<td>The RealPresence Resource Manager system public key, which in the public key system is distributed widely, and is not kept secure.</td>
</tr>
<tr>
<td>CRL Info</td>
<td>The date by which the current certificate revocation list must be replaced by a new list and the version of the list.</td>
</tr>
</tbody>
</table>
If you are waiting for a previous request to be signed, click **No**. Because the RealPresence Resource Manager system currently supports only one identity certificate, only the most recent private key is retained. The digital certificate resulting from the most recent CSR is the only certificate that will match the retained private key and is therefore the only identity certificate that can be installed.

If this is a new certificate signing request, click **Yes** to continue.

3 In the **Certificate Information** dialog box, enter the identifying information for your RealPresence Resource Manager system and click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name</td>
<td>Two-letter (ASCII only) ISO 3166 country code in which the server is located.</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>Full state or province name (ASCII only) in which the server is located.</td>
</tr>
<tr>
<td>Locality Name</td>
<td>City name (ASCII only) in which the server is located.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Enterprise name (ASCII only) at which the server is located.</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>Subdivision (ASCII only) of the enterprise at which the server is located.</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>The host name of the system (read-only), as defined in the network settings.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>The IPv4 address of the system (read-only), as defined in the network settings.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>When applicable, the IPv6 address of the system, as defined in the network settings.</td>
</tr>
<tr>
<td>Email Address</td>
<td>E-mail address (ASCII only) for a contact at the enterprise.</td>
</tr>
</tbody>
</table>

A **File Download** dialog box appears.

4 In the **File Download** dialog box, click **Save**.

5 In the **Save As** dialog box, enter a unique name for the file, browse to the location to which to save the file, and click **Save**.

6 Submit the file (or text within the file) as required by your certificate authority.

When your certificate authority has processed your request, it sends you a signed digital certificate for your RealPresence Resource Manager system. Some certificate authorities send only the signed digital certificate while others send all of the certificates that form the chain of trust.
(including intermediate and/or root CA certificates). These certificates may arrive as e-mail text, e-mail attachments, or be available on a secure web page.

**Install a Certificate**

This procedure describes how to install a certificate or certificate chain provided by a certificate authority. It assumes that you’ve received the certificate or certificate chain in one of the formats accepted by the RealPresence Resource Manager system. See “Certificates Accepted by the RealPresence Resource Manager System” on page 448.

---

**Warning**

Installing certificates requires a system restart and terminates all active conferences.

When you install a certificate, the change is made to the certificate store immediately, but the system can't implement the change until it restarts and reads the changed certificate store.

---

**To install a signed certificate that identifies the RealPresence Resource Manager system**

1. Go to Admin > Management and Security > Certificate Management and click **Install Certificates**.

   A warning appears stating that changes made to the certificates will require a system restart to take effect.

2. In the **Add Certificates** dialog box, do one of the following:
   - If you have a PFX, P7B, or single certificate file, click **Upload certificate**, enter the password (if any) for the file, and browse to the file or enter the path and file name.
   - If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box below. You can paste multiple PEM certificates one after the other.

3. Click **OK**.

   If you are uploading a signed identity certificate for the first time, it will replace the RealPresence Resource Manager system self-signed certificate.

4. If you are uploading a signed identity certificate for the first time, you can verify that the new signed certificate has replaced the default self-signed certificate:
   - In the list of certificates, select the **Resource Manager self-signed certificate** and click **View Certificate Details**.
   - When the **Certificate Details** dialog box appears, verify that the information in the **Issued To** and **Issued By** sections has been replaced by the signed public certificate from the certificate authority.
c Click OK to close the dialog box.

Upload a Certificate Revocation List

This section describes how to install a certificate revocation list (CRL) provided by a certificate authority.

The RealPresence Resource Manager system requires a CRL for each CA or sub-CA in the certificate chain. The system also requires that you upload a new CRL at regular intervals. This interval can be as short as a few days in higher security environments or a few months in environments with lower security requirements.

To upload a certificate revocation list

2 In the Select file dialog box, browse to the location of the CRL that you obtained from the CA and select the file.
3 Click Open.

Delete a Certificate

You can delete certificates from the system, but the RealPresence Resource Manager system prevents you from deleting any certificate that breaks the identity certificate’s chain of trust. To delete these certificates, new CA certificates must be installed and the identity certificate must be replaced.

Removing certificates requires a system restart, which terminates all active conferences.

When you remove a certificate, the change is made to the certificate store immediately, but the system can’t implement the change until it restarts and reads the changed certificate store.

To delete a certificate

1 Admin > Management and Security > Certificate Management.

The Certificate Management page displays the list of currently available certificates.
Select the certificate to be deleted and click **Delete Certificate**. A warning appears stating that changes made to the certificates will require a system restart to take effect.

3 Click **Yes** to continue.

4 When prompted, click **Yes** to confirm the deletion. A dialog box informs you that the certificate has been deleted.

**View the Expiration Dates for Certificates and CRLs**

Certificates and certificate revocation lists expire. To view their expiration dates, see “View Certificates and Certificate Details” on page 450.

**Change the System User Interface Timeout and Number of Sessions**

To change the system user interface timeout and number of sessions

1 Go to **Admin > Management and Security Settings > Session Management**.

2 On the **Session Management** page, configure these settings as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable remote access connections</td>
<td></td>
</tr>
<tr>
<td>Resource Manager user interface timeout</td>
<td>By default, the RealPresence Resource Manager system user interface times out after 10 minutes of inactivity. Use this procedure to change the timeout value for the user interface inactivity timer. Possible value is 5 to 60 minutes.</td>
</tr>
<tr>
<td>Maximum number of sessions per user</td>
<td>The number of simultaneous login sessions per user ID. By default, the maximum number of sessions per user ID is 5. Possible value is 1 to 10 sessions.</td>
</tr>
</tbody>
</table>
Give Enterprise Users Default Scheduler Role

By default when local users are added to the RealPresence Resource Manager system, they are assigned the Scheduler role. By default, when you integrate a RealPresence Resource Manager system to an Active Directory, enterprise users are not assigned a role. In this case, you must either assign each enterprise user a role, or you can use this procedure to give enterprise users the Scheduler role by default.

To give enterprise users default Scheduler role for a RealPresence Resource Manager system

1. Go to Admin > Management and Security Settings > Session Management.
2. Mark the Associate non-local Resource Manager users with basic scheduler role by default check box.
3. Click Update.

Change the Message for Enterprise Users without a Role

To change the message enterprise users without a role see when they try to log into a RealPresence Resource Manager system

1. Go to Admin > Management and Security Settings > Session Management.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of sessions per system</td>
<td>The number of simultaneous login sessions by all users. By default, the maximum number of sessions by all users is 50. Possible value is 2 to 50 sessions.</td>
</tr>
<tr>
<td>Note</td>
<td>If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to arrive is granted access, and the system terminates the non-Administrator session that's been idle the longest.</td>
</tr>
</tbody>
</table>
2 Edit the Message to be displayed to unauthorized users.
   For example, enter a message such as “Your username and password are valid, but you have no permissions on this system. Contact your IT department for more information.”

3 Click Update.

**Control Remote Connections to the System**

By default, users can access the RealPresence Resource Manager system remotely. You can disable this ability.

To control RealPresence Resource Manager system access with Remote Desktop Connection

1 Go to Admin > Management and Security Settings > Session Management.

2 Clear the Enable remote access connections option.

3 Click Update.
Automatic Registration Synchronization

You can configure the RealPresence Resource Manager system to send registration server addressing information for the global directory server (GDS) when the endpoint is registered to the RealPresence Resource Manager system.

For the RealPresence Resource Manager system, the GDS is the same as the global address book (GAB).

This automatic registration synchronization service only works for endpoints that register with the GDS or are manually added to the RealPresence Resource Manager system after the Automatic Registration Synchronization setting is enabled.

So if the Automatic Registration Synchronization setting is enabled and an endpoint registers with the GDS, the GDS addressing information is sent to the endpoint. If the Automatic Registration Synchronization setting is enabled and an endpoint is added manually to the RealPresence Resource Manager system, the GDS addressing information is sent to the endpoint.

If automatic discovery and configuration is not successful, you can manually add endpoints.

- **Automatic Registration Synchronization** works only for endpoints that register with the Global Directory Server after the setting is enabled; it does not automatically register pre-existing endpoints.
- The RealPresence Resource Manager system only supports Automatic Registration Synchronization for Polycom and selected third-party endpoints operating in standard mode. For supported endpoint types, including third-party endpoint types, see “Endpoint Types” on page 87.

To enable Automatic Registration Synchronization of endpoints


2. In the Automatic Registration Synchronization section of the Endpoint Management Settings page, select Synchronize endpoint registration and click Update.

   After you have changed this setting, all endpoints you add are automatically provisioned.
Set Common Passwords for Endpoints

The **Common Password** feature allows you to manage endpoints that have the same global administrative password. However, it cannot reset the administrative password on endpoints.

If you use the **Common Password** feature, access to password-protected data within endpoints is granted if the specified common password matches the endpoints’ **Administrator Password**.

### To set common passwords for endpoints

1. Go to **Admin > Management and Security Settings > Endpoint Management Settings**.
2. In the **Common Password** section of the **Endpoint Management Settings** page, select **Use a Common Password**.
3. Enter the common **User Name** and the common password in the **Password** and **Verify Password** fields and click **Update**.

---

Leave these settings blank if your Polycom endpoints require individual passwords or do not have passwords. To configure a global administrative password for all Polycom endpoints, use scheduled provisioning.

Disable Common Password for Endpoints

### To disable common passwords for endpoints

1. Go to **Admin > Management and Security Settings > Endpoint Management Settings**.
2. In the **Common Password** section of the **Endpoint Management Settings** page, clear **Use a Common Password** and click **Update**.

The common password feature is disabled. However, the values for the common password feature are retained in the database, so it can be easily re-enabled.
Set Local Account Lockout and Timeout

To set local account lockout and timeout

1. Go to Admin > Management and Security Settings > Local User Account Configuration.

2. On the Local User Account Configuration page, configure these settings as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout</td>
<td></td>
</tr>
<tr>
<td>Failed login threshold</td>
<td>Specify how many consecutive login failures cause the system to lock an account. Possible value is 2 to 10.</td>
</tr>
<tr>
<td>Failed login window (hours)</td>
<td>Specify the time span within which the consecutive failures must occur in order to lock the account. Possible value is 1 to 24.</td>
</tr>
<tr>
<td>Customized user account lockout duration (minutes)</td>
<td>Specify how long the user’s account remains locked. Possible value is 1 to 480.</td>
</tr>
<tr>
<td>Account Inactivity</td>
<td></td>
</tr>
<tr>
<td>Customize account inactivity threshold (days)</td>
<td>Specify the inactivity threshold that triggers disabling of inactive accounts. Possible value is 30 to 180.</td>
</tr>
</tbody>
</table>

3. Click Update.

Set Local Password Requirements

The Local Password Requirements page allows users assigned the Administrator role to change, but not disable password, security requirements by specifying password age, length, and complexity.

To set local password requirements

1. Go to Admin > Management and Security Settings > Local Password Requirements.

2. On the Local Password Requirements page, configure these settings as needed.
Add Machine Accounts

For dynamically managed endpoints associated with a room, a user assigned the Administrator or Area Administrator role must associate each room in the RealPresence Resource Manager system with a machine account. The machine account allows the room’s endpoint to connect and authenticate with the RealPresence Resource Manager system for directory and dynamic management purposes without using the endpoint user’s account.

3 Click Update.
You can setup the room and machine account the following ways:

- You can set up a machine account and create a new room at the same time, then edit the room to complete the room information.
- You can create a new room, then create the machine account and associate the machine account with the existing room. For more information, see “Add a Local Room” on page 356.

Dynamically managed HDX systems also require a machine account for each HDX that the RealPresence Resource Manager system will manage. The machine account allows the endpoint to connect and authenticate with the RealPresence Resource Manager system for dynamic management purposes without using the endpoint user’s account.

The **Add Machine Account** dialog box includes the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Machine Account</td>
<td>Select or clear this option to enable and disable (respectively) the machine account you create for the endpoint.</td>
</tr>
<tr>
<td>Unlock Machine Account</td>
<td>Select this option to unlock machine accounts that become locked when they exceed the Failed login threshold. This will only happen when the password expires.</td>
</tr>
<tr>
<td>User ID</td>
<td>Enter a unique name for the machine account. As a best practice, name the machine account in a way that associates it with the corresponding device. For example, if your company names endpoint systems for the system user or room (for example, bsmith_HDX or Evergreen_Room), then give the machine account an associated User ID (bsmith_HDX_machine or evergreen_room_machine).</td>
</tr>
<tr>
<td>Password/Confirm Password</td>
<td>Enter a password for the machine account user ID. This password must meet the Local Password Requirements. This password expires in 365 days.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a meaningful description for the endpoint.</td>
</tr>
<tr>
<td>Associate with an existing user or room</td>
<td>Select this option to associate the endpoint system with a specific user or room. This may be a local or enterprise user or room.</td>
</tr>
<tr>
<td>Associate with a new room (created automatically)</td>
<td>Select this option to associate the endpoint system with a system-generated room. The name of the new room is the same as the machine account User Name and can be edited when you edit the room.</td>
</tr>
<tr>
<td>Assign Area</td>
<td>When areas are enabled, you can assign the newly-created room to an area. Only users who manage more than one area can assign areas.</td>
</tr>
</tbody>
</table>
Once you have created this machine account on the RealPresence Resource Manager system, provide this information to the appropriate HDX system administrator. They should enter this **User ID** and **Password** as the **User Name** and **Password** on the HDX **Provisioning Service** page.

Note that the machine account password expires after one year. After the expiration, the HDX login will fail. After three failed login attempts, the system locks the machine account. You can reset the password and unlock the machine account by editing it and assigning a new password.

**To add a machine account**

1. Go to **Admin > Management and Security Settings > Machine Accounts**.
2. Click **Add**.
3. In the **Add Machine Account** dialog box, complete the fields.
4. Click **OK**.

**Change Database Passwords**

The RealPresence Resource Manager system uses five user names to access its database. You can change the passwords for those user names to comply with any requirements you may have to change passwords on a regular basis.

You also use the user listed as **PlcmDbo** if you should need to reformat your internal database. For more information, see “**Reformat the Existing Database**” on page 438.

The system will restart after you change these passwords. Make sure that you use this function when no conferences are active or scheduled.

**To change internal database passwords**

1. Go to **Admin > Management and Security Settings > Database Security**.
2. Select the database user whose password you want to change.
3. Click **Change Password**.
4. In the Change Database User Password dialog, enter the new password in the **New Password** and **Confirm New Password** fields.

   If you want the system to generate a password, click **Create Password**. Be sure to write down the password that displays.

5. Click **OK**.
6 Click **Apply Password Changes**.

The system resets the passwords and restarts. It may take the RealPresence Resource Manager system up to 10 minutes to shut down and then restart all server processes.
Setting Up Site Topology

This chapter describes how to edit the default Polycom Resource Manager system topology settings to support your company’s site topology. It includes these topics:

• “Site Topology Set Up” on page 467
• “Managing Sites” on page 477
• “Site Link Operations” on page 491
• “Site-to-Site Exclusions” on page 494
• “Territories” on page 496
• “Network Clouds” on page 497

Site Topology Set Up

Note
If your RealPresence Resource Manager is integrated with a Polycom DMA system, the DMA system inherits all site topology settings from the Resource Manager. Be sure to consult with your DMA system admin before making any changes, see “Considerations for Site Topology” on page 251.

Site topology information describes your network and its interfaces to other networks, including the following elements:

- **Site** — A local area network (LAN) that generally corresponds with a geographic location such as an office or plant. A site contains one or more network subnets, so a device’s IP address identifies the site to which it belongs.

- **Network clouds** — A Multi-protocol Label Switching (MPLS) network cloud defined in the site topology. An MPLS network is a private network that links multiple locations and uses label switching to tag packets with origin, destination, and quality of service (QoS) information.
Note that MPLS clouds are not associated with an IP address ranges, so they can be used to group multiple subnets. They could also represent a service provider.

While links to MPLS clouds have bandwidth and bit rate limitations, the cloud is infinite. In this way, clouds reflect the way in which businesses control bandwidth and bit rate.

- **Internet/VPN** — A entity that represents your network’s connection to the public Internet.
- **Site link** — A network connection between two sites or between a site and an MPLS network cloud.
- **Site-to-site exclusion** — A site-to-site connection that the site topology doesn’t permit an audio or video call to use.
- **Territory** — A grouping of one or more sites for which a Resource Manager system is responsible.

The site topology you create within the Resource Manager system should reflect your network design. Consider the following information and best practices when creating your site topology:

- If your RealPresence Resource Manager is integrated with a Polycom DMA system, the DMA system inherits all site topology settings from the Resource Manager. Be sure to consult with your DMA system admin before making any changes, see “Considerations for Site Topology” on page 251.

- If possible, connect all sites to an MPLS cloud. MPLS clouds are like corporate networks, used to connect multiple subnets in multiple sites, but all servicing a company.

- Avoid cross loops or multiple paths to a site; otherwise a call may have different paths to a single destination. The more cross, circular, and multi paths you have, the higher the number of calculations for a conference.

- Link sites that aren’t connected to an MPLS cloud directly to another site that is connected to an MPLS cloud. Do not create orphan sites.

- Calls are routed through a bridge, so bandwidth and bit rate limits for the site and subnet apply to all calls made using that bridge.

- Reserve the Internet/VPN “site” for IP addresses that fall outside your private or corporate network (for example remote workers), because all calls routed to the Internet/VPN site will be routed through the site on your private or corporate network that has Internet access.
The Resource Manager system site topology function uses a dynamic, embedded mapping tool that graphically displays the sites, clouds (network and Internet), and site links (site-to-site or site-to-cloud) in your network.

Within this global and graphical view of the video conferencing network, you can:

- Create and link up to 500 sites
- Zoom and pan to view specific network components
- View system and device alarms
- View the video network capacity for sites and site links as indicated by the color and shape of its icons.
- Filter the view by site name, territory name, IP address, network devices, and alerts

**Sites List**

The Sites page (Admin > Topology > Sites) contains a list of the sites defined to the Resource Manager system.

Use the commands in the Actions list to add a site, edit or delete existing sites, and see information about a site, including the number of devices of each type it contains.

The following table describes the fields in the Sites list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the site.</td>
</tr>
</tbody>
</table>
Add/Edit Site Dialog Box

Use the Add Site dialog box to define a new site in the Resource Manager system’s site topology and specify which subnets are associated with it. Use the Edit Site dialog box to redefine information for an existing site.

The following table describes the fields in the Add Site and Edit Site dialog boxes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Site Name</td>
<td>A meaningful name for the site. The name can be up to 64 characters long, and may include spaces, dashes, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description (ASCII only) of the site.</td>
</tr>
<tr>
<td>Site with RPAD</td>
<td>This functionality not supported in this release.</td>
</tr>
<tr>
<td>Enable Mutual TLS</td>
<td>Enable Mutual TLS</td>
</tr>
</tbody>
</table>
### Setting Up Site Topology

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override ITU Dialing Rules</td>
<td>Check this box to override the standard dial rules established by the International Telecommunications Union.</td>
</tr>
<tr>
<td>PBX Access Code</td>
<td>The access code required to enter the site’s PBX system.</td>
</tr>
<tr>
<td>Country Code</td>
<td>The country code for the country in which the site is located.</td>
</tr>
<tr>
<td>Area Code</td>
<td>The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.</td>
</tr>
<tr>
<td># of Digits in Subscriber Number</td>
<td>The number of digits in a phone number. For example, in the United States, subscriber numbers may have seven digits or ten digits depending upon the region.</td>
</tr>
<tr>
<td>Assignment Method</td>
<td>The ISDN number assignment method for the site. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Auto Assignment.</strong> Select this option when ISDN numbers are not assigned to IP devices.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DID (Direct Inward Dial).</strong> Select this option when you assign a range of phone numbers received from the telephone company service.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Gateway Extension Dialing.</strong> Select this option when you have a single gateway phone number and a range of extensions (E.164 aliases) that are internal to the company. In this case, calls go through a gateway. Endpoints are differentiated by the extension at the end of the dial string.</td>
</tr>
<tr>
<td></td>
<td>When a site is assigned an automatic assignment method, devices without an ISDN number are assigned one when they register. These numbers allow inbound calls to reach specific video endpoints. After an ISDN number is assigned to an endpoint, it is reserved for use as long as that endpoint remains registered with the Resource Manager system.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not assign ISDN numbers automatically, you cannot call IP-only endpoints through an ISDN line.</td>
</tr>
<tr>
<td>Territory</td>
<td>Assigns the site to a territory, and thus to a Resource Manager system.</td>
</tr>
<tr>
<td>Location</td>
<td>Specify the geographic location of the site either by longitude+latitude or country+city.</td>
</tr>
</tbody>
</table>
### Assigned Area
Available only when areas are enabled.
The area to which the site is assigned.
A user can only view area-specific information for an area(s) that he has permission to manage.

### Total Bandwidth (Mbps)
The total bandwidth of the pipe at the site.

### Call Max Bit Rate (kbps)
The maximum bandwidth that can be used for each intrasite call at the site. The default and maximum value is 2000000 (2 GB).

### ISDN Number Assignment—Assignment Method = DID (Direct Inward Dial)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># Digits in Call Line Identifier</td>
<td>Enter the number of digits in the Call Line Identifier (CLID), which is the dialed number. The maximum is 17.</td>
</tr>
<tr>
<td></td>
<td>• For example, in the United States, the number of digits in the CLID is often 7 for outside local calls, 4 for internal calls, or 11 for callers in a different area code.</td>
</tr>
<tr>
<td></td>
<td>• This number indicates what part of the full dial string is sent to the gatekeeper for address resolution.</td>
</tr>
<tr>
<td># Digits in Short Phone Number</td>
<td>Enter the number of digits in the short form of the dialing number.</td>
</tr>
<tr>
<td></td>
<td>• For example, in the United States, internal extensions are usually four or five digits.</td>
</tr>
<tr>
<td></td>
<td>• This number indicates what part of the dial string is sent to the gatekeeper for address resolution in gateway + extension dialing.</td>
</tr>
<tr>
<td>ISDN Number Range - Start</td>
<td>The starting ISDN number to assign automatically to IP devices.</td>
</tr>
<tr>
<td>ISDN Number Range - End</td>
<td>The ending ISDN number to assign automatically to IP devices.</td>
</tr>
</tbody>
</table>

### ISDN Number Assignment—Assignment Method = Gateway Extension Dialing

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Phone Number</td>
<td>Phone number of the site gateway.</td>
</tr>
<tr>
<td>E164 Start</td>
<td>• The starting number in a range of available extensions to assign automatically to IP devices.</td>
</tr>
<tr>
<td></td>
<td>• When a device without native ISDN registers, a number within the start and end range is assigned, so that the device can be called through an ISDN line.</td>
</tr>
<tr>
<td>E164 End</td>
<td>The ending number in the range of available extensions to assign automatically to IP devices.</td>
</tr>
</tbody>
</table>
### Setting Up Site Topology

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H.323 Routing</strong></td>
<td></td>
</tr>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables call routing through the Internet.</td>
</tr>
<tr>
<td>Allowed via H.323 aware firewall</td>
<td>Enables call routing through the Internet, using an H.323-aware firewall.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For an outbound call to the Internet, you must enter the firewall gateway</td>
</tr>
<tr>
<td></td>
<td>service (e.g. a Polycom VBP appliance) code before the IP address in the</td>
</tr>
<tr>
<td></td>
<td>dial string.</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Allowed via H.323 aware firewall</strong> you must create a site</td>
</tr>
<tr>
<td></td>
<td>link between this site and the Internet/VPN site.</td>
</tr>
<tr>
<td>Allowed via H.323 aware SBC or ALG</td>
<td>Enables call routing via the Internet, using an H.323-aware SBC (Session</td>
</tr>
<tr>
<td></td>
<td>Border Control) or ALG (Application Level Gateway) server.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For an outbound call to the Internet, you must enter the firewall gateway</td>
</tr>
<tr>
<td></td>
<td>service (for example, a Polycom VBP appliance) code before the IP address</td>
</tr>
<tr>
<td></td>
<td>in the dial string.</td>
</tr>
<tr>
<td>Call Signaling IP Address</td>
<td>IP address of the SBC or ALG server. Supports only IPv4 addresses.</td>
</tr>
<tr>
<td>Port</td>
<td>Port address of SBC or ALG server.</td>
</tr>
<tr>
<td>Send Unmodified Dial String to SBC/ALG</td>
<td>Select this option if your SBC or ALG requires that the original dial</td>
</tr>
<tr>
<td></td>
<td>string is passed to it. For example, an H.323 Annex O dial string such</td>
</tr>
<tr>
<td></td>
<td>as <a href="mailto:user@company.com">user@company.com</a> is passed directly to the SBC or ALG instead of</td>
</tr>
<tr>
<td></td>
<td>resolving company.com to an IP address.</td>
</tr>
<tr>
<td></td>
<td>Deselect this option if your equipment requires a dial string that is</td>
</tr>
<tr>
<td></td>
<td>converted from company.com to gatekeeper IP address. This option is</td>
</tr>
<tr>
<td></td>
<td>appropriate for the Polycom VBP.</td>
</tr>
<tr>
<td><strong>SIP Routing</strong></td>
<td></td>
</tr>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables call routing through the Internet.</td>
</tr>
</tbody>
</table>

---

*Notes*

- For an outbound call to the Internet, you must enter the firewall gateway service (e.g. a Polycom VBP appliance) code before the IP address in the dial string.
- If you select **Allowed via H.323 aware firewall** you must create a site link between this site and the Internet/VPN site.

*Note*

For an outbound call to the Internet, you must enter the firewall gateway service (for example, a Polycom VBP appliance) code before the IP address in the dial string.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed via SIP aware firewall</td>
<td>Enables call routing through the Internet, using an SIP-aware firewall.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes</strong></td>
</tr>
<tr>
<td></td>
<td>• For an outbound call to the Internet, you must enter the firewall gateway service (e.g. a Polycom VBP appliance) code before the IP address in the dial string.</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Allowed via SIP aware firewall</strong> you must create a site link between this site and the Internet/VPN site.</td>
</tr>
<tr>
<td>Allowed via SIP aware SBC or ALG</td>
<td>Enables call routing via the Internet, using an SIP-aware SBC (Session Border Control) or ALG (Application Level Gateway) server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>For an outbound call to the Internet, you must enter the firewall gateway service (for example, a Polycom VBP appliance) code before the IP address in the dial string.</td>
</tr>
<tr>
<td>Call Signaling IP Address</td>
<td>IP address of the SBC or ALG server. Supports only IPv4 addresses.</td>
</tr>
<tr>
<td>Port</td>
<td>Port address of SBC or ALG server.</td>
</tr>
<tr>
<td><strong>Subnets</strong></td>
<td></td>
</tr>
<tr>
<td>Subnet IP Address/Mask</td>
<td>Specifies the subnets within the site. For each subnet, includes:</td>
</tr>
<tr>
<td></td>
<td>• IP Address range</td>
</tr>
<tr>
<td></td>
<td>• Subnet mask</td>
</tr>
<tr>
<td></td>
<td>• Maximum bandwidth for the subnet</td>
</tr>
<tr>
<td></td>
<td>• Maximum bit rate per call for the subnet</td>
</tr>
<tr>
<td><strong>Enterprise Directory Settings—Endpoint Enterprise Directory security group settings</strong></td>
<td></td>
</tr>
<tr>
<td>Universal Security Group Filter</td>
<td>When in secure mode, search and select groups that are provisioned to the endpoints to represent the valid lists of users that can log in as a user or administrator. If a user is not a member of one of the selected groups then the user is denied access to the endpoint.</td>
</tr>
<tr>
<td>Enterprise Directory Admin Group</td>
<td></td>
</tr>
<tr>
<td>Enterprise Directory User Group</td>
<td></td>
</tr>
</tbody>
</table>
Site Links

The Site Links page lists the links defined in the site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud (see “Network Clouds” on page 102).

Use the commands in the Actions list to add, edit, or delete a site link. See “Add/Edit Site Link Dialog Box” on page 475 for a description of the fields in the site list.

Add/Edit Site Link Dialog Box

Use the Add Site Link dialog box to define a new site link in the Resource Manager system’s site topology. Use the Edit Site Link dialog box to redefine an existing site link. A site link can connect two sites, or it can connect a site to an MPLS network cloud.

The following table describes the fields in the Add Site Link and Edit Site Link dialog boxes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A meaningful name for the site (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the site (up to 200 characters).</td>
</tr>
<tr>
<td>From site</td>
<td>The originating site of the link. The drop-down list includes all defined sites and the Internet. Can’t be changed for a site-to-cloud link.</td>
</tr>
<tr>
<td>To site</td>
<td>The destination site of the link. The drop-down list includes all defined sites and an Internet/VPN option. Can’t be changed for a site-to-cloud link.</td>
</tr>
<tr>
<td>Total bandwidth (Mbps)</td>
<td>Specifies the total bandwidth limit for this link.</td>
</tr>
<tr>
<td>Call Max bit rate (kbps)</td>
<td>Specifies the per-call bandwidth limit for this link.</td>
</tr>
</tbody>
</table>

Site-to-Site Exclusions

The Site-to-Site Exclusions page contains a list of the direct site-to-site connections that the system won’t permit a call or session to use.

Use the commands in the Actions list to add and delete site-to-site exclusions. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From/To Site</td>
<td>Name of one of the two sites connected by the excluded link.</td>
</tr>
<tr>
<td>To/From Site</td>
<td>Name of the other site.</td>
</tr>
</tbody>
</table>
Territories

The Territories page contains a list of the territories defined in the site topology. On the right, it displays information about the selected territory.

A territory is a set of one or more sites for which a Resource Manager system is responsible. By default, there is one territory named Default Resource Manager Territory, and its primary node (the Resource Manager system responsible for it) is set to this system.

Use the commands in the Actions list to add, edit, or delete a territory. See “Add/Edit Territory Dialog Box” on page 476 for a description of the fields in the territory list.

Add/Edit Territory Dialog Box

Use the Add Territory dialog box to define a new territory in the Resource Manager system’s site topology. Use the Edit Territory dialog box to define a new territory in the Resource Manager system’s site topology.

The following table describes the fields in the Add Territory and Edit Territory dialog boxes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Territory Info</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the territory (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the territory (up to 200 characters).</td>
</tr>
<tr>
<td>Primary Node</td>
<td>The primary node of the Resource Manager system responsible for this territory.</td>
</tr>
<tr>
<td>Backup Node</td>
<td>The second node, if any, of the Resource Manager system responsible for this territory.</td>
</tr>
<tr>
<td>Associated Sites</td>
<td></td>
</tr>
<tr>
<td>Search Sites</td>
<td>Enter search string or leave blank to find all sites.</td>
</tr>
<tr>
<td>Search Result</td>
<td>Lists sites found and shows the territory, if any, to which each currently belongs. Select a site and click the right arrow to move it to the Selected Sites list.</td>
</tr>
<tr>
<td>Selected Sites</td>
<td>Lists sites selected and shows the territory, if any, to which each currently belongs.</td>
</tr>
</tbody>
</table>
Network Clouds

The Network Clouds page contains a list of the MPLS (Multi-protocol Label Switching) network clouds defined in the site topology.

Use the commands in the Actions list to add, edit, or delete an MPLS cloud. See the Cloud Info section of the “Add/Edit Network Cloud Dialog Box” on page 477 for a description of the fields in the Network Clouds list.

Add/Edit Network Cloud Dialog Box

Use the Add Network Cloud dialog box to define a new MPLS network cloud in the Resource Manager system’s site topology. Use the Edit Network Cloud dialog box to redefine an existing MPLS network cloud.

The following table describes the fields in the Add Network Cloud and Edit Network Cloud dialog boxes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Info</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the cloud (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the cloud (up to 200 characters).</td>
</tr>
<tr>
<td>Linked Sites</td>
<td></td>
</tr>
<tr>
<td>Search Sites</td>
<td>Enter search string or leave blank to find all sites.</td>
</tr>
<tr>
<td>Search Result</td>
<td>Lists sites found and shows the territory, if any, to which each belongs.</td>
</tr>
<tr>
<td></td>
<td>Select a site and click the right arrow to open the Add Site Link dialog box.</td>
</tr>
<tr>
<td>Selected Sites</td>
<td>Lists sites linked to the cloud and shows the territory, if any, to which each belongs.</td>
</tr>
</tbody>
</table>

Managing Sites

Site operations include:

- “View the Graphical Site Topology” on page 478
- “View the Sites List” on page 478
- “Add a Site” on page 479
- “View Site Information” on page 488
- “Assign Locations to a Site” on page 488
- “Edit Site Settings” on page 490
View the Graphical Site Topology

To view the graphical site topology

>> Go to Admin > Topology > Site Topology.

The Site Topology page appears. It graphically displays the sites and site links defined to the Resource Manager system.

— Hover over a map element to view information about it.
— Use the slider bar to zoom in or out on the map.
— Select or deselect elements (Site Links, Bandwidth, or Site Names) to change what is displayed on the map.
— Use the Select Sites drop-down list to filter (by site name, territory name, IP address, network devices, and alerts) which sites are displayed on the map.

View the Sites List

To view the Sites list

>> Go to Admin > Topology > Sites.

The Sites list appears. It includes this information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the site.</td>
</tr>
<tr>
<td>Country Code</td>
<td>The country code for the country in which the site is located.</td>
</tr>
<tr>
<td>Area Code</td>
<td>The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.</td>
</tr>
<tr>
<td>Max Bandwidth (Mbps)</td>
<td>The total bandwidth limit for audio and video calls.</td>
</tr>
</tbody>
</table>
Add a Site

To add a site

1. Go to Admin > Topology > Sites or Admin > Topology > Site Topology.
2. In the Sites list or Site Topology page, click Add Site.
3. In the Add Site dialog box, enter a Site Name and Description for the site.
4. Complete the General Info, Routing, Subnet, and if applicable ISDN Number Assignment, sections of the Add Site dialog box. The minimum information required is Site Name, Description, Location, and Subnets.
   For information about all of the site fields, see “Add/Edit Site Dialog Box” on page 470.
5. Click OK.
   The new site is added to the system and the Edit Site Provisioning dialog box appears. These are the site-based parameters that the Resource Manager system automatically provisions to endpoint systems operating in dynamic management mode.
6. As needed, edit the default site provisioning details and click Apply.

**Note**

Not all of the site provisioning parameters apply to all endpoint systems being provisioned. If an endpoint system does not have a corresponding parameter, it ignores the parameter.

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and Time Settings</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Specify the country code for their location.</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems at the site being provisioned...</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Date Format</td>
<td>Specify the date display format.</td>
</tr>
<tr>
<td>Auto Adjust for Daylight Saving Time</td>
<td>Specify whether or not to adjust the endpoint’s system clock for daylight savings time.</td>
</tr>
<tr>
<td>Time Format</td>
<td>Specify the time display format.</td>
</tr>
</tbody>
</table>
| Time Server                               | Specify whether to connect to a time server for automatic system time settings.  
Select Auto to require that the video endpoint system synchronize with an external time server that is identified by a network domain controller. Because it is identified by a network domain controller, you do not need to enter the IP address of the time server.  
Select Manual to require that the video endpoint system synchronize with an external time server that may not be identified by a network domain controller. In this case, you must also enter the IP address of the time server in the Time Server Address field.  
If Time Server is set to Off, or if the Time Server is set to Manual or Auto but the endpoint system cannot connect to the time server, the date and time must be manually reset at the endpoint. |
| Primary Time Server Address               | Specify the address of the primary time server when Time Server is set to Manual.                                                                                                                                                                                                                                                                                                         |
| Secondary Time Server Address             | Specify the address of the secondary time server when Time Server is set to Manual.                                                                                                                                                                                                                                                                                                       |
| Timezone                                  | Specify the time difference between GMT (Greenwich Mean Time) and the endpoint system’s location.                                                                                                                                                                                                                                                                                   |
| Firewall Settings                         | Specify whether to define the TCP and UDP ports.  
• If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting.  
• If the firewall is not H.323 compatible, enable this setting. The endpoint systems will assign a range of ports starting with the TCP and UDP ports you specify. The endpoint system defaults to a range beginning with port 3230 for both TCP and UDP.  
**Note**  
You must open the corresponding ports in the firewall. You must also open the firewall’s TCP port 1720 to allow H.323 traffic. |
| Start TCP Port                            | Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.  
**Note**  
You must also open the firewall’s TCP port 1720 to allow H.323 traffic.                                                                                                                                                                                                                                                                 |
| Start UDP Port                            | Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.                                                                                                                                                                                                 |
| Enable H.460 Firewall Traversal          | Allows the endpoint system to use H.460-based firewall traversal. For more information, see the Administrator’s Guide for Polycom HDX Systems.                                                                                                                                                                                                                                         |
### Setting Up Site Topology

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Configuration</td>
<td>Specify whether the endpoint systems should determine the NAT Public WAN Address automatically.</td>
</tr>
<tr>
<td></td>
<td>• If the endpoint systems are behind a NAT that allows HTTP traffic, select <strong>Auto</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If the endpoint systems are behind a NAT that does not allow HTTP traffic, select <strong>Manual</strong>. Then specify a <strong>NAT Public (WAN) Address</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If the endpoint systems are not behind a NAT or are connected to the IP network through a virtual private network (VPN), select <strong>Off</strong>.</td>
</tr>
<tr>
<td>NAT Public (WAN) Address</td>
<td>When <strong>NAT Configuration</strong> is set to <strong>Manual</strong>, specify the address that callers from outside the LAN should use to call the endpoint systems.</td>
</tr>
<tr>
<td>NAT is H.323 Compatible</td>
<td>Specify that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.</td>
</tr>
<tr>
<td>Address Displayed in Global Directory</td>
<td>Specify whether to include the endpoint system’s information in the global directory</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Private</strong> to exclude the endpoint from the global directory</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Public</strong> to include the endpoint in the global directory</td>
</tr>
<tr>
<td>Enable SIP Keep Alives</td>
<td>When checked, SIP Keep Alive messages are enabled.</td>
</tr>
<tr>
<td>H323 Settings</td>
<td></td>
</tr>
<tr>
<td>Enable IP H.323</td>
<td>Specify whether to enable IP H.323 calls.</td>
</tr>
<tr>
<td>Gatekeeper IP Address</td>
<td>When <strong>Use Gatekeeper</strong> is set to <strong>Specify</strong>, enter the gatekeeper IP address in this field.</td>
</tr>
<tr>
<td>Use Gatekeeper for Multipoint Calls</td>
<td>Specify whether multipoint calls use the endpoint system’s internal multipoint capability or the Polycom MCU’s Conference on Demand feature. This feature is available only if the system is registered with a PathNavigator.</td>
</tr>
<tr>
<td>SIP Settings</td>
<td></td>
</tr>
<tr>
<td>Enable SIP</td>
<td>Specify whether to enable SIP calls.</td>
</tr>
<tr>
<td>Automatically Discover SIP Servers</td>
<td>The Resource Manager system will issue a DNS query to locate the SIP server and provision that information to endpoints.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Specify the IP address or DNS name of the SIP proxy server for the network.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Specify the IP address or DNS name of the SIP registrar server for the network.</td>
</tr>
<tr>
<td></td>
<td>• In an Microsoft Office Communications Server 2007 or Microsoft Lync Server 2010 environment, specify the IP address or DNS name of the Office Communications Server or Lync Server server.</td>
</tr>
<tr>
<td></td>
<td>• If registering a remote HDX system with an Office Communications Server Edge Server or Lync Server Edge Server, use the fully qualified domain name of the access edge server role.</td>
</tr>
<tr>
<td>Backup Proxy Server</td>
<td>Specify the IP address or DNS name of a backup SIP proxy server for the network.</td>
</tr>
<tr>
<td>Backup Registrar Server</td>
<td>Specify the IP address or DNS name of a backup SIP registrar server for the network.</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems at the site being provisioned...</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Transport Protocol**                      | Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure determines which protocol is required.  
  • Auto enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments.  
  • TCP provides reliable transport via TCP for SIP signaling.  
  • UDP provides best-effort transport via UDP for SIP signaling.  
  • TLS provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060.                                                                                     |
| **SIP Server Type**                         | Specify the type of the SIP registrar server.  
  You can provision the following SIP registrar servers:  
  • Polycom (DMA system)  
  • BroadSoft (BroadWorks)  
  • Cisco (Cisco Unified Communications Manager)  
  • Avaya (Avaya Communications Manager)  
  • Siemens (OpenScape UC Server)  
  • Microsoft (Lync of Office Communications Server) |
| **Verify Certificate**                      | Enable this option when the endpoint system’s certificate should be verified by the certificate authority.                                                                                                                                                                                                                                                                                                                                                     |
| **Use Resource Manager Provisioning Credentials** | Enable this option when the endpoint system should use the credentials the user entered at the endpoint to use for authenticate when registering with a SIP registrar server.                                                                                                                                                                                                                      |
| **Common SIP User Name**                    | Specify the name to use for authentication when registering with a SIP registrar server, for example, msmith@company.com. If the SIP proxy requires authentication, this field and the password cannot be blank.                                                                                                                                                                                                                         |
| **Common SIP Password**                     | Specify the password that authenticates the system to the registrar server.                                                                                                                                                                                                                                                                                                                                                                                         |
| **Provisioning Settings**                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Provisioning Polling Interval (minutes)     | Specify the frequency at which the endpoint systems poll the Resource Manager system for new provisioning information.  
  By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes. There is no maximum value enforced. When the value of this interval is set to 0, the endpoint systems do not poll the Resource Manager system for new provisioning information.                                                                 |
| Software Update Polling Interval (minutes)  | Specify the frequency at which the endpoint systems poll the Resource Manager system for a new software update package.  
  By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes. There is no maximum value enforced. When the value of this interval is set to 0, the endpoint systems do not poll the Resource Manager system for a new software update package.                                                                                           |
<p>| <strong>Quality of Service Settings</strong>             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Type of Service</td>
<td>Specify the IP Precedence or Diffserv value for video packets.</td>
</tr>
<tr>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>Audio Type of Service</td>
<td>Specify the IP Precedence or Diffserv value for audio packets.</td>
</tr>
<tr>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>FECC Type of Service</td>
<td>Specify the IP Precedence or Diffserv value for Far End Camera Control packets.</td>
</tr>
<tr>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>Type of Service Field</td>
<td>Specify the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control:</td>
</tr>
<tr>
<td></td>
<td>• IP Precedence — Represents the priority of IP packets sent to the system. The value can be between 0 and 5.</td>
</tr>
<tr>
<td></td>
<td>• Diffserv — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.</td>
</tr>
<tr>
<td>Maximum Transmission Unit Size (bytes)</td>
<td>Specify the Maximum Transmission Unit (MTU) size used in IP calls. If the video becomes blocky or network errors occur, packets may be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets may be too small; increase the MTU.</td>
</tr>
<tr>
<td>Enable PVEC</td>
<td>Allows the endpoint system to use PVEC (Polycom Video Error Concealment) if packet loss occurs. PVEC delivers smooth, clear video over IP networks by concealing the deteriorating effects of packet loss</td>
</tr>
<tr>
<td>Enable RSVP</td>
<td>Allows the endpoint system to use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. Both the near site and far site must support RSVP in order for reservation requests to be made to routers on the connection path.</td>
</tr>
<tr>
<td>Enable Dynamic Bandwidth</td>
<td>Specify whether to let the endpoint system automatically find the optimum line speed for a call.</td>
</tr>
<tr>
<td>Maximum Transmit Bandwidth (Kbps)</td>
<td>Specify the maximum transmission line speed.</td>
</tr>
<tr>
<td>Maximum Receive Bandwidth (Kbps)</td>
<td>Specify the maximum reception line speed.</td>
</tr>
</tbody>
</table>

### Security Settings

<table>
<thead>
<tr>
<th>Security Profile</th>
<th>Read-only field. Displays the security level of the Resource Manager system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Room Password for Remote Access</td>
<td>Specify whether the local endpoint system password and remote access password are the same.</td>
</tr>
<tr>
<td>Room Password</td>
<td>Enter or change the local endpoint system password here. When the local password is set, you must enter it to configure the system Admin Settings using the remote control. The local password must not contain spaces.</td>
</tr>
<tr>
<td>Administrator ID</td>
<td>Enter the administrative account that should be used to access the endpoint system remotely.</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems at the site being provisioned...</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Remote Access Password</strong></td>
<td>For endpoint systems, enter or change the remote access password here. When the remote access password is set, you must enter it to upgrade the software or manage the endpoint systems from a computer. The remote access password cannot include spaces.</td>
</tr>
<tr>
<td><strong>Meeting Password</strong></td>
<td>Specify the password users must supply to join multipoint calls on this endpoint system if the call uses the internal multipoint option, rather than a bridge. This field can also be used to store a password required by another endpoint system that this system calls. If a password is stored in this field, you do not need to enter it at the time of the call; the endpoint system supplies it to the system that requires it. The meeting password cannot include spaces.</td>
</tr>
<tr>
<td><strong>Enable Secure Mode</strong></td>
<td>Specify whether to operate in secure mode (also known as security mode), which uses TLS, HTTPS, AES, digital signatures, and other security protocols, algorithms, and mechanisms. These protocols encrypt management communication over IP, preventing access by unauthorized users. When devices at a site are provisioned to operate in secure mode, the Resource Manager system can only perform the dynamic management operations of automatic provisioning, automatic software update, and directory and presence services for the devices. The Resource Manager system cannot perform monitoring or control operations for the devices. For more information, see the Administrator’s Guide for Polycom HDX Systems.</td>
</tr>
<tr>
<td><strong>AES Encryption</strong></td>
<td>Specify how to encrypt calls with other sites that support AES encryption. • <strong>Off</strong>—No encryption is used. • <strong>When Available</strong>—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don’t support it. • <strong>Required for Video Calls Only</strong>—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are allowed. Video endpoints must support AES Encryption to participate in the call. • <strong>Required for All Calls</strong>—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are not allowed. All endpoints must support AES Encryption to participate in the call.</td>
</tr>
<tr>
<td><strong>Enable Web Access</strong></td>
<td>Specify whether to allow remote access to the endpoint system by the web. <strong>Note</strong> The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the Web Access Port setting to disable the port.</td>
</tr>
<tr>
<td><strong>Enable Telnet Access</strong></td>
<td>Specify whether to allow remote access to the system by Telnet. <strong>Note</strong> The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the Web Access Port setting to disable the port.</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems at the site being provisioned...</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Enable SNMP Access          | Specify whether to allow remote access to the system by SNMP.  
|                             | **Note**                                                |
|                             | The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the **Web Access Port** setting to disable the port. |
| Web Access Port             | Specify the port to use when accessing the endpoint system’s web interface.  
|                             | If you change this from the default (port 80), specify a port number of 1025 or higher, and make sure the port is not already in use. You will need to include the port number with the IP address when you use the Polycom HDX web interface to access the system. This makes unauthorized access more difficult.  
|                             | **Note**                                                |
|                             | The system restarts if you change the web access port. |
| Allow Video Display On Web  | Specify whether to allow viewing of the room where the endpoint system is located, or video of calls in which the endpoint system participates, using the endpoint system’s web interface.  
|                             | **Note**                                                |
|                             | This feature activates both near site and far site video displays in Web Director. |
| NTLM Version                | Specify the NTLM version the endpoint system should use to authenticate. |

<table>
<thead>
<tr>
<th>Security Settings 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Session Timeout in Minutes</td>
<td>When sessions are enabled, Specify the number of minutes your system can be idle before the session times out.</td>
</tr>
<tr>
<td>Lock Port after Failed Logins</td>
<td>Specify the number of failed login attempts allowed before the system locks the account. If set to Off, the system will not lock the user account due to failed login attempts. This selection controls local and web interface login attempts. For example, if you select 3 here, a user who fails to log in properly twice on the web interface and twice on the local interface is locked out on the fourth attempt.</td>
</tr>
<tr>
<td>Failed Login Window in Hours</td>
<td>Specify the amount of time that the account remains locked due to failed login attempts.</td>
</tr>
<tr>
<td>Port Lock Duration in Minutes</td>
<td>Specify the amount of time that the port remains locked due to failed login attempts.</td>
</tr>
<tr>
<td>Maximum Peer Certificate Chain Depth</td>
<td>Specify how many links a certificate chain can have. The term peer certificate refers to any certificate sent by the far-end host to the HDX system when a network connection is being established between the two systems.</td>
</tr>
<tr>
<td>Verify Certificates for all Web Access</td>
<td>Specify whether the endpoint requires certificate validation to access the endpoint.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Whitelist</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Whitelist of IPs</td>
<td>When a whitelist is enabled, allows access to an endpoint’s web interface only by those systems with an IP address that matches a pattern using regular expression notation.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
</table>

#### Enter all IPs allowed to Connect via the web

Specify (by IP addresses using regular expression notation) which systems can access an endpoint’s web interface. Addresses are matched by pattern, which means that you could allow IP address that you did not mean to allow. For example, if you entered an IP address of 15.1.2.111, all of the following results would match:

- 15.1.2.111
- 15.182.1.11
- 15.1.252.111

If you want to allow a range of IP addresses, use the * wildcard instead. For example, enter `10.11.*.*` to allow all IP addresses that begin with 10.11.

#### General Settings

<table>
<thead>
<tr>
<th>Heartbeat Posting Interval (minutes)</th>
<th>Specify the frequency at which the endpoint systems poll the Resource Manager system for a heartbeat.</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Call Stats Posting Interval (minutes)</td>
<td>Specify the frequency at which the endpoint systems poll the Resource Manager system for in call statistics.</td>
</tr>
</tbody>
</table>

#### Calendaring Settings

| Automatically Discover Exchange Server | Specify that the Resource Manager system should discover the Microsoft Exchange server for the site by searching DNS records. |
| Specify Exchange Server | Specify that the Resource Manager system should use the Microsoft Exchange server specified in the Exchange Server Address field. |
| Exchange Server Address | Specify the IP address or DNS name of the Microsoft Exchange server for the site. |

#### Enterprise Directory Settings

| Group Display Name | Specify whether the Resource Manager system should identify groups by their common name (cn) or their DisplayName. These names are extracted from the Active Directory. |
| User Display Name | Specify whether the Resource Manager system should identify users by their common name (cn) or their DisplayName. These names are extracted from the Active Directory. |
| Enterprise Directory Admin Group | Specify the Active Directory group whose members should have access to the Admin settings on the HDX system. This name must exactly match the name in the Active Directory server for authentication to succeed. |
| Enterprise Directory User Group | Specify the Active Directory group whose members should have access to the User settings on the HDX system. This name must exactly match the name in the Active Directory server for authentication to succeed. |

#### Directory Settings

| Use Default Directory Server This Server | When the Specify radio button is marked, you can use the Directory Server field enter the IP address of the directory server you wish to use. |
### Field
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Certificate</td>
<td></td>
</tr>
<tr>
<td><strong>Presence Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Use Presence Directory Server</td>
<td></td>
</tr>
<tr>
<td>This Server</td>
<td></td>
</tr>
<tr>
<td>Specify</td>
<td>When the Specify radio button is marked, you can use the <strong>Presence Server</strong> field enter the IP address of the presence server you wish to use.</td>
</tr>
<tr>
<td>Verify Certificate</td>
<td></td>
</tr>
</tbody>
</table>
View Site Information

To view information about an existing site
1. Go to Admin > Topology > Sites or Admin > Topology > Site Topology.
2. In the Sites list or Site Topology page, select the site of interest and click Site Information.

The Site Information dialog box displays the following site information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the site.</td>
</tr>
<tr>
<td>Location</td>
<td>The specified location of the site identified either by longitude + latitude or by country + city.</td>
</tr>
<tr>
<td>Bandwidth (Mbps)</td>
<td>The specified total bandwidth limit for audio and video calls.</td>
</tr>
<tr>
<td>Bandwidth Used</td>
<td>Identifies the percentage of the maximum bandwidth currently occupied with audio and video calls.</td>
</tr>
<tr>
<td>Device Types</td>
<td>Identifies the type (Bridges, DMAs, VBPs, and Endpoints) and number of devices assigned to the site.</td>
</tr>
<tr>
<td>Alarms</td>
<td>Identifies the device alarms present within the site. Alarm information includes Status, Device Name, Device Type, and Description. Click Details to view more device details.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Identifies the subnets within the site. Subnets information includes Bandwidth Used, Subnet (name), and (maximum) Bandwidth.</td>
</tr>
</tbody>
</table>

Assign Locations to a Site

Location has not always been a required field for sites. If your existing sites do not include location information, use the Assign Locations action to update your sites.

To assign a location to an existing site
1. Go to Admin > Topology > Sites or Admin > Topology > Site Topology.
2. Click Assign Locations.
3. In the Assign Locations to Sites dialog box, select the site of interest by marking the associated check box and click Specify Location.
4 To specify a location by city name:
   a From the Enter Location By drop-down list, select Search for City.
   b If you know it, select the Country name for the location.
   c Enter the name of the City and click Search.
      The system returns the list of cities that match your entry.
   d Select the appropriate city using the Country, Division, and Subdivision fields to identify it and click Select.

5 To specify a location by latitude and longitude in decimal degrees format:
   a From the Enter Location By drop-down list, select Latitude/Longitude (Decimal format).
   b Enter the Latitude and Longitude coordinates in decimal degrees (for example, Baltimore has a latitude of 39.3° and a longitude of 76.6°).
   c Enter a Location Name. The system uses this location name for reference only; it does not validated the location name against the latitude and longitude coordinates that you enter.
   d Select the Country name for the location and click Select.
      The system uses the coordinates you input to place the site in the proper location on its site topology map.

6 To specify a location by latitude and longitude in DaysMinutesSeconds format:
   a From the Enter Location By drop-down list, select Latitude/Longitude (DDD:MM:SS format).
   b Enter the Latitude and Longitude coordinates in the required format and select
   c Enter a Location Name. The system uses this location name for reference only; it does not validated the location name against the latitude and longitude coordinates that you enter.
   d Select the Country name for the location and click Select.
      The system uses the coordinates you input to place the site in the proper location on its site topology map.
Edit Site Settings

**Note**
Changing network topology may affect the accuracy of reports based on this information. To retain historical data for the current network topology, generate reports before making changes.

If your RealPresence Resource Manager is integrated with a Polycom DMA system, the DMA system inherits all site topology settings from the Resource Manager. Be sure to consult with your DMA system admin before making any changes, see “Considerations for Site Topology” on page 251.

To edit settings for a site

1. Go to Admin > Topology > Sites or Admin > Topology > Site Topology.
2. In the Sites list or Site Topology page, select the site of interest and click Edit Site.
3. Edit the General Info, Site Routing, Site Subnet, and if applicable ISDN Number Assignment, sections of the Edit Site dialog box. For information about these sections, see “Add/Edit Site Dialog Box” on page 470.
4. Click OK.

Edit Site Provisioning Settings

To edit the site provisioning settings for a site

1. Go to Admin > Topology > Sites or Admin > Topology > Site Topology.
2. In the Sites list or Site Topology page, select the site of interest and click Edit Site Provisioning Details.
3. As needed, edit the site provisioning details and click Apply. For information about these details, see “Add/Edit Site Dialog Box” on page 470.
4. Click OK.
Delete a Site

**Note**
Devices that belonged to a deleted site are automatically reassigned to support Internet and VPN calls.

**To delete a site**

1. Go to Admin > Topology > Sites or Admin > Topology > Site Topology.
2. In the Sites list or Site Topology page, select the site of interest and click Delete.
3. Click Yes to confirm the deletion.

Site Link Operations

When you add a site link, you enter the starting and ending sites of the link and the maximum bandwidth and bit rates available for calls (audio and video) that use the link. Links are bidirectional. After you have created a link from Site A to Site B, you automatically have a bi-directional link from Site B to Site A, although the link appears as unidirectional.

**Note**
The bit rate can be set at the network level, the device level, and the conference level. If there is a discrepancy between these bit rate settings, the system implements the lowest bit rate setting. The only exception, is that the bit rate in the RMX profile takes precedence over the bit rate in the conference settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name (ASCII only) of the inter-site link.</td>
</tr>
<tr>
<td>Description</td>
<td>Description (ASCII only of the inter-site link.</td>
</tr>
<tr>
<td>From Site</td>
<td>Identifies the first site to be linked. The drop-down list includes all defined sites and the Internet.</td>
</tr>
<tr>
<td>To Site</td>
<td>Identifies the other site to be linked. The drop-down list includes all defined sites and an Internet/VPN option.</td>
</tr>
<tr>
<td>Total Bandwidth (kbps)</td>
<td>The maximum available bandwidth for audio and video calls, which you set at the gateway or router.</td>
</tr>
<tr>
<td>Call Max Bit Rate (kbps)</td>
<td>The maximum bit rate allowed for an audio and video call.</td>
</tr>
</tbody>
</table>
Site-link operations include:

- “View the Site Links List” on page 493
- “Add a Site Link” on page 493
- “Edit a Site Link” on page 493
- “Delete a Site Link” on page 494
Setting Up Site Topology

View the Site Links List

To view the Site Links list

>> Go to Admin > Topology > Site-Links.

The Site-Links list appears.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the link</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the link</td>
</tr>
<tr>
<td>From Site</td>
<td>First site reached in the call route</td>
</tr>
<tr>
<td>To Site</td>
<td>Final site reached through this call link</td>
</tr>
<tr>
<td>Max Bandwidth</td>
<td>The maximum available bandwidth for audio and video calls, which you set at the gateway or router. Only applies to direct links.</td>
</tr>
<tr>
<td>Max Bit Rate (kbps)</td>
<td>The maximum bit rate allowed for an audio and video call. Only applies to direct links.</td>
</tr>
</tbody>
</table>

Add a Site Link

Before you can create a site link, you must add two or more sites to the system.

To add a site link

1. Go to Admin > Topology > Site-Links.
2. In the Site-Links page, click Add.
3. In the Add Site-Link dialog box, enter a Name and Description for the link and select the starting (From Site) and ending (To Site) sites.
4. Enter the Bandwidth and Max Bit Rate and click Save.

The new link appears on the Site Links page.

Edit a Site Link

You may need to edit site links when network changes are made.

If you make a bandwidth change, the current load is not affected; however, the bandwidth available for future conferences may be affected.
To edit a site link
1. Go to Admin > Topology > Site-Links.
2. In the Site-Links list, select the link of interest and click Edit.
3. In the Edit Site-Link dialog box, edit the Name, Description, Bandwidth or Max Bit Rate.
4. Click Save.

Delete a Site Link

You can remove site links from the Polycom Resource Manager system.

Note
Avoid removing a link on which a scheduled conference depends.

To delete a site link
1. Go to Admin > Topology > Site-Links.
2. In the Site-Links list, select the site link of interest and click Delete.
3. Click Yes to confirm the deletion.

Site-to-Site Exclusions

Create site-to-site exclusions to explicitly deny connection between two sites for audio or video calls.

Site-link exclusion operations include:
- View the Site-to-Site Exclusion List
- Add a Site-to-Site Exclusion
- Edit a Site-to-Site Exclusion
- Delete a Site-to-Site Exclusion

View the Site-to-Site Exclusion List

To view the Site-to-Site exclusion list
>> Go to Admin > Topology > Site-to-Site Exclusion.

The Site-to-Site Exclusions list appears.
Add a Site-to-Site Exclusion

Before you can create a site link exclusion, you must add two or more sites to the system.

Exclusions are by definition bilateral. No call traffic is allowed to flow across the site-link in either direction.

To add a site-to-site exclusion
1. Go to Admin > Topology > Site-to-Site Exclusions.
2. In the Site-to-Site Exclusions page, click Add.
3. In the Add Site-to-Site Exclusions wizard:
   a. Select the first site of the From/To site pair (by clicking the appropriate button). If needed, use the Search Site field to find the site.
   b. Select the second site of the From/To site pair (by enabling the appropriate check box) and click Continue. You can select more than one site, if needed.
   c. Review the site-to-site exclusion and if it is correct, click Save Exclusion.

Edit a Site-to-Site Exclusion

You cannot edit a site-to-site exclusion; you can only delete it and then re-add it.

Delete a Site-to-Site Exclusion

To delete a site-to-site exclusion
1. Go to Topology > Site-to-Site Exclusions.
2. In the Site-to-Site Exclusions page, select the exclusion of interest and click Delete.
3. Click Yes to confirm the deletion.
Territories

A territory is a set of one or more sites for which a Resource Manager system is responsible. By default, there is one territory named Default Resource Manager Territory, and its primary node (the Resource Manager system responsible for it) is set to this system. For more information, see “Territories” on page 496.

Territory operations include:
• “View the Territory List” on page 496
• “Add a Territory” on page 496
• “Edit a Territory” on page 496
• “Delete a Territory” on page 497

View the Territory List

To view the Territories list

Go to Admin > Topology > Territories.

The Territories list appears.

Add a Territory

To add a territory

1 Go to Admin > Topology > Territories.
2 In the Territories page, click Add.
3 Complete the Territory Info and Associated Sites sections of the Add Territories dialog box. For information about these fields, see “Add/Edit Territory Dialog Box” on page 476.
4 Click OK.

Edit a Territory

To edit a territory

1 Go to Admin > Topology > Territories.
2 In the Territories page, select the territory of interest and click Edit.
3 Change the **Territory Info** and **Associated Sites** information of the Add Territories dialog box as needed. For information about these fields, see “Add/Edit Territory Dialog Box” on page 476.

4 Click **OK**.

**Delete a Territory**

To delete a territory

1 Go to **Admin > Topology > Territories**.
2 In the **Territories** page, select the territory of interest and click **Delete**.
3 Click **Yes** to confirm the deletion.

**Network Clouds**

To simplify the network topology, define network clouds to represent a hub with many sites connected to each other such as a private network or VPN.

Network cloud operations include:

- “Multi-tenancy Considerations for Network Clouds” on page 497
- “View the List of Network Clouds” on page 497
- “Add a Network Cloud” on page 498
- “Edit a Network Cloud” on page 498
- “Delete a Network Cloud” on page 499

**Multi-tenancy Considerations for Network Clouds**

When areas are enabled for your system, sites can be assigned to areas. You must be sure that each site within a network cloud belongs to the same area. View the Sites list to determine the area for a site, see “View the Sites List” on page 478.

**View the List of Network Clouds**

To view the Network Cloud list

>> Go to **Admin > Topology > Network Clouds**.

The **Network Clouds** list appears.
### Add a Network Cloud

**To add a network cloud**

1. Go to Admin > Topology > Network Clouds.
2. In the Network Clouds page, click Add.
3. In the Cloud Info section of the Add Network Cloud dialog box, enter a unique and meaningful Name and Description for the cloud.
4. To create a link between a site and the network cloud:
   a. Click Linked Sites.
   b. In the Search Sites field, enter all or part of the site name or location and click Find.
      - The list of sites containing the search phrase appear in the Search Results column.
   c. Select one or more sites to link with the network cloud and then click the right arrow to move them to the Selected Sites column.
5. Click OK.

### Edit a Network Cloud

**To edit a network cloud**

1. Go to Admin > Topology > Network Clouds.
2. In the Network Clouds page, select the network cloud of interest and click Edit.
3. Edit the Cloud Info or to create a link between a site and the network cloud:
   a. Click Linked Sites.
   b. In the Search Sites field, enter all or part of the site name or location and click Find.
      - The list of sites containing the search phrase appear in the Search Results column.
   c. Select one or more sites to link with the network cloud and then click the right arrow to move them to the Selected Sites column.
4. Click OK.
Delete a Network Cloud

To delete a network cloud

1. Go to Admin > Topology > Network Clouds.

2. In the Network Clouds page, select the network cloud of interest and click Delete.

3. Click Yes to confirm the deletion.
This chapter describes how to configure the Polycom® RealPresence® Resource Manager system to send alerts to users via E-mail for specific types of system and endpoint events. It includes these topics:

- “Set Up Remote Alerts” on page 501
- “Edit a Remote Alert Profile” on page 509
- “Disable a Remote Alert Profile” on page 510
- “Delete a Remote Alert Profile” on page 510
- “Disable Remote Alerts” on page 510

**Set Up Remote Alerts**

The RealPresence Resource Manager system remote alerts functionality is very flexible. It allows you to:

- Assign different severity levels to different classifications of RealPresence Resource Manager system and Endpoint alerts.
- Create different alert profiles so that different types of alerts can be sent to different people. So if you have administrators who specialize by device type (for example bridges, endpoints, or servers), you can create profiles that notify each type of administrator of failures related to those specific types of devices.

To set up remote alerts, you must complete the following tasks:

1. “Set Up RealPresence Resource Manager System-generated E-mail Account” on page 503.
4. Set Endpoint Alert Level Settings.
5  “Add a Remote Alert Profile” on page 507.
6  “Associate a Remote Alert Profile With a User” on page 509.
Set Up RealPresence Resource Manager System-generated E-mail Account

To set the RealPresence Resource Manager system-generated E-mail account
1. Go to Admin > Server Settings > E-mail.
2. On the E-mail page, enter the E-mail account (ASCII only) from which the Resource Manager system will send conference notification E-mails and system alerts.
3. Specify the IP address of the mail server from which the RealPresence Resource Manager system will send conference notification E-mails.

- Many E-mail servers will block or discard E-mails without a qualified From: address. To avoid this issue, make sure each person with Scheduler permissions has a valid E-mail address.
- Many E-mail servers will block or discard E-mails from untrusted domains, in which case you may need to change the default RealPresence Resource Manager system E-mail address to one in a trusted domain.

4. Click Update.

Enable RealPresence Resource Manager System Remote Alerts

To enable RealPresence Resource Manager system remote alerts
1. Go to Admin > Server Settings > Remote Alert Setup.
3. Set a Remote Alert quiescent time, which is the amount of time (in minutes) the system should wait after alerts have been detected but not cleared before starting the alert notification process, and if applicable, the remote alert notification process.
4. Click Update.
Set RealPresence Resource Manager System Remote Alert Level Settings

The RealPresence Resource Manager system monitors and reports events regarding its performance, connections, and services. It categorizes alerts into three alert levels: **Info**, **Minor**, or **Major**.

By default the Alert Severity Level is set to Info for all of the **Resource Manager Alert Types** it reports. You have these options:

- You can leave all of the Alert Severity Levels set to **Info** and create a single remote alert profile that allows you to notify all users assigned that profile about system events of all types.
- You can change some of the Alert Severity Levels to either **Minor** or **Major** and create multiple remote alert profiles that notify different users of system events of different types and severity levels.

**To set the RealPresence Resource Manager system remote alert level settings**

1. Go to **Admin > Alert Settings > Resource Manager Alert Level Settings**.
2. On the **Resource Alert Level Settings** page, change the Alert Severity Level for the following **Resource Manager Alert Type** system events, as required.

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Alert indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Down</td>
<td>A Polycom MCU has failed.</td>
</tr>
<tr>
<td>Database Connection Down</td>
<td>The connection to the database has been lost.</td>
</tr>
<tr>
<td>Enterprise Directory Connection Down</td>
<td>The connection to the enterprise directory server has been lost.</td>
</tr>
<tr>
<td>Enterprise Directory System Account Password Failure</td>
<td>The connection to the enterprise directory server could not be established because the account password was incorrect.</td>
</tr>
<tr>
<td>Resource Manager Failover Occurred</td>
<td>(In redundant RealPresence Resource Manager system configurations only.) The system has failed over from one system server to the other.</td>
</tr>
<tr>
<td>License Capacity Threshold Exceeded</td>
<td>The number of available seats defined by the installed license is within 5% of the total license capacity.</td>
</tr>
<tr>
<td>License Expired Warning</td>
<td>The license will expire in less than 30 days.</td>
</tr>
<tr>
<td>Bridge Time Discrepancy</td>
<td>A difference between the clock on the Polycom MCU and the RealPresence Resource Manager system clock.</td>
</tr>
</tbody>
</table>
Setting Up Remote Alerts

3 Click **Update**.

**Set Endpoint Alert Level Settings**

Monitored endpoints send events to the RealPresence Resource Manager system. The RealPresence Resource Manager system categorizes and reports endpoint alerts into three alert levels: **Info**, **Minor**, or **Major**.

By default the **Alert Severity Level** is set to **Info** for all of the **Endpoint Alert Types** it reports. You have these options:

- You can leave all of the **Alert Severity Levels** set to **Info** and create a remote alert profile for each endpoint type being monitored that allows you to notify all users assigned that profile about all endpoint events applicable to that endpoint type.

- You can change some of the **Alert Severity Levels** to either **Minor** or **Major** and create multiple remote alert profiles that notify different users of endpoint events of different types and severity levels.

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Alert indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant Server Down</td>
<td>(In redundant RealPresence Resource Manager system configurations only.) The connection or synchronization between the primary and secondary server has been lost.</td>
</tr>
<tr>
<td>Redundancy Service Stopped</td>
<td>(In redundant RealPresence Resource Manager system configurations only.) The redundancy service has stopped.</td>
</tr>
<tr>
<td>Resource Manager Failover Occured</td>
<td>The primary server failover occured.</td>
</tr>
<tr>
<td>Site Bandwidth Threshold Exceeded</td>
<td>The site bandwidth threshold, which is set at 90% of capacity, has been exceeded.</td>
</tr>
<tr>
<td>Subnet Bandwidth Threshold Exceeded</td>
<td>The subnet bandwidth threshold, which is set at 90% of capacity, has been exceeded.</td>
</tr>
<tr>
<td>Site Link Bandwidth Threshold Exceeded</td>
<td>The site link bandwidth threshold, which is set at 90% of capacity, has been exceeded.</td>
</tr>
<tr>
<td>Certificate Expiration Warning</td>
<td>The specified certificate will expire in 30 days. If the certificate is not renewed within 30 days, the alert continues daily.</td>
</tr>
<tr>
<td>Certificate Expired Warning</td>
<td>The specified certificate has expired. The alert continues daily until the certificate is renewed or removed.</td>
</tr>
<tr>
<td>Database Backup Failure</td>
<td>The database backup has failed.</td>
</tr>
</tbody>
</table>
To set the endpoint alert level settings

1. Go to Admin > Alert Settings > Endpoint Alert Level Settings.

2. On the Endpoint Alert Level Settings page, change the Alert Severity Level for the different types of endpoint events as required.

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Alert indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Control</td>
<td>The battery in the endpoint’s remote needs to be replaced.</td>
</tr>
<tr>
<td>Battery Low</td>
<td></td>
</tr>
<tr>
<td>Credentials Required</td>
<td>The endpoint system requires that the user enter a valid username and password.</td>
</tr>
<tr>
<td>Credentials Failed</td>
<td>An attempt to log into the endpoint system failed.</td>
</tr>
<tr>
<td>HTTP Forbidden</td>
<td>The endpoint must be used in https: mode only.</td>
</tr>
<tr>
<td>Device Not Responding</td>
<td>The endpoint is not responding to the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Heartbeat Timeout</td>
<td>The endpoint did not send a heartbeat to the RealPresence Resource Manager system within the required timeout period.</td>
</tr>
<tr>
<td>Gatekeeper Status Unknown</td>
<td>The system gatekeeper cannot determine the connection status of the endpoint.</td>
</tr>
<tr>
<td>Gatekeeper Rejected</td>
<td>The gatekeeper rejected the endpoint’s attempt to register.</td>
</tr>
<tr>
<td>Gatekeeper Unregistered</td>
<td>The endpoint is not registered to the gatekeeper.</td>
</tr>
<tr>
<td>Directory Status Unknown</td>
<td>The system gatekeeper cannot determine the directory status of the endpoint.</td>
</tr>
<tr>
<td>Directory Not Registered</td>
<td>The endpoint is not registered to the directory service.</td>
</tr>
<tr>
<td>Presence Status Unknown</td>
<td>The system gatekeeper cannot determine the presence status of the endpoint.</td>
</tr>
<tr>
<td>Presence Unregistered</td>
<td>The endpoint is not registered to the presence service.</td>
</tr>
<tr>
<td>User Assistance Request</td>
<td>The endpoint user sent a request for help.</td>
</tr>
</tbody>
</table>
Setting Up Remote Alerts

Add a Remote Alert Profile

You can add a remote alert profile to identify which device alerts from which devices should be sent as part of a remote alert profile. Note that using a combination of setting alerts by device type and by specific types, provide additional granularity in managing device alerts.

To add a remote alert profile

1. Go to Admin > Alert Settings > Remote Alert Profiles.
3. In the Add Remote Alert Profile dialog box, enter a Name and Description for the profile.
4. To activate the profile, mark the Enabled check box.
5 Configure one of the following:

- To have all RealPresence Resource Manager system alerts sent as part of this profile, select Info, Minor, and Major.

- To have a subset of RealPresence Resource Manager system alerts sent as part of this profile, select any combination of Info, Minor, or Major. These selections work in conjunction with the RealPresence Resource Manager system alert level settings you chose previously.

- To have no RealPresence Resource Manager system alerts sent as part of this profile, leave Info, Minor, and Major cleared.

6 To use the device type to identify which devices and device alerts should be sent as part of this profile, click Alert by Device Type and configure one of the following. For endpoint systems, these selections work in conjunction with the endpoint alert level settings you choose previously.

a To have all device alerts for all device types sent as part of this profile, in the Device Type Alert Level Mapping page, select Info, Minor, and Major for all of the device types.

b To have a subset of device alerts for all device types sent as part of this profile, in the Device Type Alert Level Mapping page, select any combination of Info, Minor, or Major for each device type.

c To have all device alerts for a subset of device types sent as part of this profile, in the Device Type Alert Level Mapping page, select Info, Minor, or Major for each device type to be included in the profile. Alerts for those device types that do not have an alert level selected will not be included.

7 To use the device name to identify which devices and device alerts should be sent as part of this profile, click Alert by Device.

- If you set device alerts for specific devices, these settings override settings made on the Alert by Device Type page. The settings are not cumulative.
- You cannot set the system up to send device alerts for specific desktop video endpoints. Polycom CMA Desktop and Polycom PVX endpoints are not displayed in the Available Device list.

a As needed, use the Filter to customize the device list.

b In the Available Devices list, select the devices to add to the profile. Use Ctrl to select multiple devices.

c Click the down arrow to add the devices to the Monitored Devices list and configure one of the following:

» To have all device alerts for all selected devices sent as part of this profile, for the devices in the Monitored Devices list, select Info, Minor, and Major for each device.
» To have a subset of device alerts for all selected devices sent as part of this profile, for the devices in the **Monitored Devices** list, select any combination of **Info**, **Minor**, or **Major** for each device.

» To have all device alerts for a subset of device types sent as part of this profile, for the devices in the **Monitored Devices** list, select **Info**, **Minor**, and **Major** for each device to be included in the profile. Alerts for those devices in the **Monitored Devices** list that do not have an alert level selected will not be included.

8  Click OK.

### Associate a Remote Alert Profile With a User

**To associate a remote alert profile with a user**

1  Go to **User > Users**.

2  To search for a user:
   
   a  In the **Search** field of the **Users** page, search for the user of interest.

   Searches for a user on the RealPresence Resource Manager system **Users** page are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

   b  To search both local and enterprise users, clear the **Local Users Only** check box and press **Enter**.

   The first 500 users in the database that match your search criteria are displayed in the **Users** list.

   c  If the list is too large to scan, further refine your search string.

3  Select the user of interest and click **Edit User**.

4  In the **Edit User** dialog box, click **Associated Alert Profile**.

5  Select the **Remote Alert Profile** to associate with the user.

6  Click **OK**.

### Edit a Remote Alert Profile

**To edit a Remote Alert Profile**

1  Go to **Admin > Alert Settings > Remote Alert Profiles**.
2 On the Remote Alert Profiles page, select the profile of interest and click Edit Remote Alert Profile.
3 As required, edit the General Info, Alert by Device Type, and Alert by Device sections of the Edit Remote Alert Profile dialog box.
4 Click OK.

### Disable a Remote Alert Profile

**To disable a Remote Alert Profile**

1 Go to Admin > Alert Settings > Remote Alert Profiles.
2 On the Remote Alert Profiles page, select the profile of interest and click Edit Remote Alert Profile.
3 Clear Enable Profile.
4 Click Update.

### Delete a Remote Alert Profile

**To delete a Remote Alert Profile**

1 Go to Admin > Alert Settings > Remote Alert Profiles.
2 On the Remote Alert Profiles page, select the profile of interest and click Delete Remote Alert Profile.
3 Click Yes to confirm the deletion.
   - The profile is deleted from the RealPresence Resource Manager system.

### Disable Remote Alerts

**To disable all (system and device) RealPresence Resource Manager system remote alerts**

1 Go to Admin > System Settings > Remote Alert Setup.
3 Click Update.
This chapter describes the following Polycom® RealPresence® Resource Manager system operations topics:

- “Management and Maintenance Overview” on page 511
- “Recommended Regular Maintenance” on page 513

Management and Maintenance Overview

The RealPresence Resource Manager system requires relatively little ongoing maintenance beyond monitoring the status of the system and downloading backups you want to archive. All system management and maintenance tasks can be performed in the management interface. See the appropriate topic for your user role:

- Administrator Responsibilities
- Auditor Responsibilities

Administrator Responsibilities

As a RealPresence Resource Manager system administrator, you’re responsible for the installation, configuration, and ongoing maintenance of the system. You should be familiar with the following tasks and operations:

- Installing licenses when the system is first installed and when additional endpoints are added. See “Server Settings” on page 405.
- Monitoring system health and performing the recommended regular maintenance. See “Recommended Regular Maintenance” on page 513.
• Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. See “System Troubleshooting” on page 519. Should the need arise, Polycom Global Services personnel may ask you to use these tools.

• Upgrading the system when upgrades/patches are made available. See “Update the System Software” on page 447.

**Administrative Best Practices**

The following are some of our recommendations for administrative best practices:

• Perform the recommended regular maintenance.

• Except in emergencies or when instructed to by Polycom Global Services personnel, don’t reconfigure, install an upgrade, or restore a backup when there are active conferences on the system. Many of these operations will require a system restart to complete, which will result in conferences being dropped.

• Before you reconfigure, install an upgrade, or restore a backup, manually create a new backup of the system settings. Then download and archive this backup in the event that something unforeseen occurs and it becomes necessary to restore the system to a known good state.

• For proper name resolution and smooth network operations, configure at least one DNS server in your network configuration, and preferably two or more. This allows the RealPresence Resource Manager system to function properly in the event of a single external DNS failure.

• Configure at least one NTP server in your time configuration and preferably two or more. Proper time management helps ensure that your cluster operates efficiently and helps in diagnosing any issues that may arise in the future. Proper system time is also essential for accurate audit and CDR data.

**Auditor Responsibilities**

As a RealPresence Resource Manager system auditor, you’re responsible for managing the system’s logging and history retention. You should be familiar with the following configurations and operations:

• Configuring logging for the system. These settings affect the number and the contents of the log archives available for download from the system. Polycom Global Services personnel may ask you to adjust the logging configuration and/or download and send them logs.

• Configuring history retention levels for the system. These settings affect how much system activity history is retained on the system and available for download as CDRs.
Auditor Best Practices

The following are some of our recommendations for auditing best practices:

- Unless otherwise instructed by Polycom Global Services, configure logging at the production level with a rolling frequency of every day and a retention period of 60 days. If hard drive space becomes an issue, decrease the retention period incrementally until the disk space issue is resolved.
- Download log archives regularly and back them up securely (preferably offsite as well as onsite).
- Export CDRs regularly and back them up securely (preferably offsite as well as onsite).

Recommended Regular Maintenance

Perform the following tasks to keep your RealPresence Resource Manager system operating trouble-free and at peak efficiency. These tasks can be done quickly and should be run at least weekly.

Create and Archive Backups

Log into the RealPresence Resource Manager system, go to Admin > Backup System Settings and Create and Download a Backup Archive. For more information, see “Backup the System Settings” on page 515.

General System Health and Capacity Checks

On the Dashboard verify that there are no alerts indicating problems with any part of the system. For more information, see “System Dashboard” on page 321.

Certificates

Go to Admin > Management and Security > Certificate Management and verify that the list of certificates contains the certificates you’ve installed and looks as you would expect (an archived screen capture may be helpful for comparison).

Display the details for any certificate you’ve installed and verify they are as expected (an archived screen capture may be helpful for comparison). For more information, see “Manage Certificates” on page 448.

CDR export

If you want to preserve detailed call and conference history data in spreadsheet form off the RealPresence Resource Manager system, periodically download the system’s CDR (call detail record) data to your PC.
This chapter provides an overview of the Polycom® RealPresence® Resource Manager system backup and recovery procedures. It includes these topics:

- “Create System Backups” on page 515
- “Restore the System” on page 516

The backup and recovery of a RealPresence Resource Manager system includes backup and recovery of the RealPresence Resource Manager system internal database and the backup of the RealPresence Resource Manager system configuration settings.

Create System Backups

Polycom recommends creating and downloading a system archive weekly. This archive makes system restoration much simpler.

Users assigned the Administrator role can create backups of the existing system. They can create and download a system backup archive (.zip format), which includes both the database backup files and the system settings.

Backup the System Settings

This topic describes how to create a backup archive of a RealPresence Resource Manager system including system configuration settings and database files. Once the backup archive is downloaded, it can be used to restore the system to its last archived configuration after a disastrous system failure.

To backup the system settings

1. From the RealPresence Resource Manager system web interface, go to Admin > Backup System Settings.
When the Backup System Settings page appears, click Create and Download a Backup Archive.

3 In the Select location for download dialog box, enter a unique File name, browse to a location on your system and click Save.

A File Download dialog box displays the progress of the download operation.

4 When the operation is completed, click OK.

5 Browse to the location specified in step 3 and verify the file download.

**Restore the System**

A user assigned the Administrator role can restore a RealPresence Resource Manager system using a backup archive. To restore a RealPresence Resource Manager system, follow the procedures in this topic.

**To restore a system from a backup archive**

1 “Restore to Factory Default Image” on page 516.

2 Perform First Time Setup. For more information about First Time Setup, see the Polycom CMA System Getting Started Guide for this release.

3 “Restore from a Backup Archive” on page 517 using the last archived configuration. The archived configuration will overwrite the configuration that resulted from First Time Setup. The only RealPresence Resource Manager system configuration settings not included in the archive and thus not overwritten are the network settings and the security certificates required for an operational system.

In cases when the RealPresence Resource Manager system is functional, but the configuration or database is corrupted, the backup archive can also be used to return a RealPresence Resource Manager system back to its last known good archive. As long as the network settings and security certificates are operational, the last known good archive will return the RealPresence Resource Manager system to its former functional state.

**Restore to Factory Default Image**

In a disaster recovery situation, your Polycom Global Services (PGS) support representative may be required to restore your RealPresence Resource Manager system to its factory default image.

To perform this disaster recovery procedure, you will need the Restore to Factory Default DVD that shipped with the RealPresence Resource Manager system server. This DVD has the base image of the RealPresence Resource Manager system server software.
## Restore from a Backup Archive

A user with the **Administrator** role can restore the RealPresence Resource Manager system using a backup archive.

When you restore from a backup archive:

- Do not allow users to connect to the server during the restoration process.
- The system restarts when the restoration process is finished.

### To restore a backup archive

1. Go to **Admin > Backup System Settings**.
2. In the **Select Archive File** section of the **Backup System Settings** page, click ….
3. In the **Select file to upload** dialog box, select the archive file to upload and click **Open**.
4. Click **Restore from Backup Archive**.
   - Two warnings appear about the backup process. The second warns that the process is irrevocable and may result in an unusable system.
5. Click **OK**.

The system uses the archive file to restore the RealPresence Resource Manager system to the state of the backup files.

When the RealPresence Resource Manager system is functional, but the configuration or database is corrupted, you can also use these steps to return a RealPresence Resource Manager system to its last known good archive. As long as the network settings and security certificates are operational, the last known good archive will return the RealPresence Resource Manager system to its former functional state.
This chapter provides Polycom® RealPresence® Resource Manager system troubleshooting information. It includes the following topics:

- Troubleshooting Utilities Dashboard
- Troubleshooting Specific Types of Issues
  - Registration Problems and Solutions
  - Point-to-Point Calling Problems and Solutions
  - MCU and Gateway Dialing Problems and Solutions

**Troubleshooting Utilities Dashboard**

The RealPresence Resource Manager system has a Troubleshooting Utilities dashboard that brings together on one page access to all of the information you might need to diagnose system issues. It includes access to various diagnostic files and informational panes.

The diagnostic files include:

- **Traces** — Use this option to generate and download a network sniffer trace that can help you examine the traffic to and from the RealPresence Resource Manager system.

- **Resource Manager System Logs** — Use this option to generate and download a `GetAllLogs.zip` file that includes all of the RealPresence Resource Manager system log files. For more information about these system logs, see “View and Export System Log Files” on page 316.

- **Resource Manager System Report** — Use this option to generate and download a `SystemInfo.txt` file that describes the system configuration. For more information about this report, see “Resource Manager System Report” on page 318.

- **Test Network Connection** — Use this option to perform a Traceroute or Ping operation. Traceroute allows you to investigate the route path and transit times of packets as they travel across an IP network. Ping allows you to test the availability of a host on an IP network.
- **Synchronize Certificate Stores**—Use this option to reset all certificate stores with the currently uploaded certificates and certificate revocation lists (CRLs).

The information panes include:

- **Systems**—Displays summary information about the devices registered with the RealPresence Resource Manager system. For more information, see “Systems” on page 327.

- **Resource Manager Configuration**—Displays information about the configuration of the RealPresence Resource Manager system. For more information, see “Resource Manager Configuration” on page 323.

- **Resource Manager Info**—Displays general information about the RealPresence Resource Manager system. For more information, see “Resource Manager Info” on page 324.

- **Resource Manager Licenses**—Displays information about how the RealPresence Resource Manager system is licensed. For more information, see “Resource Manager Licenses” on page 325.

- **DMA**—Displays information about the Polycom DMA system as a gatekeeper.

- **Users Logged In**—Displays the type and number of users that are currently logged into the system. For more information, see “Users Logged In” on page 323.
## Troubleshooting Specific Types of Issues

This section describes information on troubleshooting specific types of issues on the Resource Manager system. It includes these topics:

- “Registration Problems and Solutions” on page 521
- “Point-to-Point Calling Problems and Solutions” on page 522
- “MCU and Gateway Dialing Problems and Solutions” on page 522

### Registration Problems and Solutions

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to place calls to an MCU conference room from a registered Polycom HDX system</td>
<td>The dynamic management mode RealPresence Resource Manager system rejects the ARQ stating that the &quot;endpoint is not registered&quot; to the gatekeeper even though the system indicates it is registered.</td>
<td>• The MCU is not registered to the gatekeeper</td>
</tr>
<tr>
<td>Some endpoints are not assigned ISDN numbers.</td>
<td>A registered H.323-only system was not assigned an ISDN number. The system could belong to a network that does not have ISDN number ranges assigned to it. No ISDN numbers are available to assign.</td>
<td>• Verify that the endpoint belongs to the site that has assigned ISDN number ranges. To do so, go to Admin &gt; Topology &gt; Sites and make sure the site has the correct ISDN range specified in the ISDN Number Assignment pane. • Verify that ISDN numbers are available to assign. • Verify that the RCF message “Can’t find ISDN free pool” from the gatekeeper returns to the endpoint.</td>
</tr>
<tr>
<td>Endpoints that were previously registered and auto-assigned ISDN numbers are being rejected when attempting to register.</td>
<td>Inconsistent configuration in ISDN number assignment has occurred.</td>
<td>• Verify that the previous ISDN range was changed.</td>
</tr>
<tr>
<td>When the Resource Manager system is restarted, some registrants that were previously online are now offline.</td>
<td>Some endpoints do not reregister when the RealPresence Resource Manager system goes down. Some MCUs do not reregister automatically after two retries.</td>
<td>• Reboot the MCU.</td>
</tr>
</tbody>
</table>
# Point-to-Point Calling Problems and Solutions

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| A call with an alias as the dial string from a registered endpoint cannot be placed to another registered endpoint. The two endpoints are in different sites. | • The site link between the sites in which the endpoints reside is not correctly defined or is missing.  
• No bandwidth is available to the site link.  
• The calling bit rate is higher than the bit rate defined in the site link.  
• ISDN alternate routing is not available.  
• Dialing rules may not be enabled or may be set to block instead of route. | • Go to Admin > Topology > Site Links and make sure that a site link exists between the two networks.  
• Make sure that the IP addresses of both endpoints are included in their respective sites.  
• If site topology is defined for both endpoints, verify that there is enough bandwidth in the site links between the two sites.  
• Verify that the dialing bit rate is lower or equal to that of the maximum bit rate defined for the site links.  
• If the endpoint is ISDN capable, verify that the ISDN parameter is correct. |

# MCU and Gateway Dialing Problems and Solutions

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| Call fails when using an MCU service. Dialing an MCU service results in a network error. | The call using the MCU service is rejected because of one of the following:  
• The MCU is not registered.  
• The MCU is offline.  
• The MCU prefix is not registered as an E.164 alias.  
• The MCU resource issue was sent through resource allocation indication or resource allocation. | • Verify that the MCU is registered.  
• Verify that the MCU is online. If the device is offline, reboot it. |
System Security and Port Usage

This section provides an overview of the port usage and security required by the Polycom® RealPresence® Resource Manager system and includes a comprehensive list of services and clients on the system that are required for normal operation. It includes these topics:

- Open Inbound Ports on the RealPresence Resource Manager System
- Outbound Ports Used by the RealPresence Resource Manager System

Open Inbound Ports on the RealPresence Resource Manager System

The following table lists the open inbound ports on the RealPresence Resource Manager system and provides a description of their use.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 80</td>
<td>HTTP web server, through which the web application displays and where Polycom endpoints post status messages</td>
</tr>
<tr>
<td>TCP/UDP 161</td>
<td>SNMP listener</td>
</tr>
<tr>
<td>TCP 389</td>
<td>Directory services (LDAP)</td>
</tr>
<tr>
<td>TCP 443</td>
<td>HTTPS web server listener</td>
</tr>
<tr>
<td>TCP 700</td>
<td>(Polycom proprietary service) Service monitor for redundant RealPresence Resource Manager system servers</td>
</tr>
<tr>
<td>TCP/UDP 1718</td>
<td>H.323 gatekeeper listener--gatekeeper discovery</td>
</tr>
<tr>
<td>TCP/UDP 1719</td>
<td>H.323 gatekeeper listener--gatekeeper statistics</td>
</tr>
<tr>
<td>TCP/UDP 1720</td>
<td>H.323 gatekeeper listener--host call</td>
</tr>
<tr>
<td>TCP 3601</td>
<td>(Polycom proprietary service) Global Address Book listener with which endpoints register</td>
</tr>
<tr>
<td>TCP 3389</td>
<td>Remote desktop</td>
</tr>
</tbody>
</table>
## Outbound Ports Used by the RealPresence Resource Manager System

The following table lists all outbound ports that the RealPresence Resource Manager system uses to communicate with other systems, including endpoints, bridges, database servers, and other network equipment.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 20</td>
<td>Used to FTP data to endpoints</td>
</tr>
<tr>
<td>TCP 21</td>
<td></td>
</tr>
<tr>
<td>TCP/UDP 24</td>
<td>Used to access the telnet interfaces on endpoints</td>
</tr>
<tr>
<td>TCP/UDP 25</td>
<td>Used to send E-mail messages to SMTP servers</td>
</tr>
<tr>
<td>TCP/UDP 53</td>
<td>Used to access domain name servers (DNS)</td>
</tr>
<tr>
<td>TCP 80</td>
<td>Used to access the web application on endpoints</td>
</tr>
<tr>
<td>TCP 135</td>
<td>Active Directory (AD) Single Signon (NetBios/NTLM)</td>
</tr>
<tr>
<td>TCP 137</td>
<td></td>
</tr>
<tr>
<td>TCP 139</td>
<td></td>
</tr>
<tr>
<td>TCP/UDP 389</td>
<td>Used to access directory (LDAP) services</td>
</tr>
<tr>
<td>TCP 443</td>
<td>Secure access to endpoint devices (SSL) including Polycom CMA Desktop.</td>
</tr>
<tr>
<td>TCP 445</td>
<td>Active Directory Single Sign-on</td>
</tr>
<tr>
<td>TCP/UDP 636</td>
<td>Used to access LDAP over TLS/SSL (LDAPS)</td>
</tr>
<tr>
<td>TCP/UDP 1719</td>
<td>Used by the gatekeeper for H.323 RAS messages</td>
</tr>
<tr>
<td>TCP/UDP 1720</td>
<td>Used by the gatekeeper for Q.931 signaling</td>
</tr>
</tbody>
</table>

Third-party port-scanning software may incorrectly identify the Polycom proprietary services as IANA-registered services, since identification is made by port number only and not by the actual protocol being transmitted.
<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/UDP 3268</td>
<td>Used to access the Microsoft Active Directory Global Catalog using StartTLS</td>
</tr>
<tr>
<td>TCP/UDP 3269</td>
<td>Used to access the Microsoft Active Directory Global Catalog using LDAP-S</td>
</tr>
<tr>
<td>TCP/UDP 3603</td>
<td>Used for HTTP communication with the Polycom PVX client</td>
</tr>
</tbody>
</table>
The RealPresence Resource Manager system enterprise MIB relates information about the system. The information is divided into these categories:

- **Configuration** — The static state of each component, for example component type, software version, current owner, values of all configured parameters.

- **Status** — The dynamic state of each component, for example the number of connections, number of conferences, number of ports (used and available), temperature, fan speed, CPU utilization, memory utilization, network link status, number of dropped packets, jitter measurements, number of successful calls, number of CPU resets.

- **Alerts** — To notify that an exception condition has occurred, for example a power supply failure, link/down up on a major interface, memory usage exceeding a predefined percentage, connections in an MCU exceeding a threshold, a logical fault or ungraceful transition.

- **Conformance** — The historical trend for selected groups of data, for example conference load over time for an MCU, bandwidth consumed over time for a network device.

---

```plaintext
POLYCOM-CMA-MIB DEFINITIONS ::= BEGIN

IMPORTS
   -- TRAP-TYPE
   FROM RFC-1215
   DateAndTime, TruthValue, TEXTUAL-CONVENTION FROM SNMPv2-TC
   MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, enterprises, Counter32,
   Integer32,Counter64 FROM SNMPv2-SMI
   ItuPerceivedSeverity FROM ITU-ALARM-TC-MIB
   InetAddressType, InetAddress, InetPortNumber FROM INET-ADDRESS-MIB
   OBJECT-GROUP, NOTIFICATION-GROUP FROM SNMPv2-CONF;

polycom MODULE-IDENTITY
LAST-UPDATED "200908130000Z"
ORGANIZATION "Polycom Inc."
CONTACT-INFO "Thomas Filarecki"
DESCRIPTION "This is the Converged Media Application (CMA) MIB."
REVISION "200908130000Z"
```
DESCRIPTION "Updated descriptions"
REVISION "200906020000Z"
DESCRIPTION "Initial draft"
::= { enterprises 13885 }

-- Object Identifiers

-- CMA configuration data

-- CMA Status data

OBJECT IDENTIFIER ::= { cma 14 }
OBJECT IDENTIFIER ::= { cma 100 }
OBJECT IDENTIFIER ::= { cma 200 }
OBJECT IDENTIFIER ::= { cma 300 }
OBJECT IDENTIFIER ::= { cmaAlertObjects 10 }
OBJECT IDENTIFIER ::= { cmaAlertObjects 20 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 10 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 20 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 30 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 40 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 50 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 60 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 70 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 80 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 90 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 110 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 120 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 130 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 140 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 150 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 160 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 170 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 180 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 190 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 200 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 210 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 220 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 230 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 240 }
OBJECT IDENTIFIER ::= { cmaConfigObjects 250 }
OBJECT IDENTIFIER ::= { cmaStatusObjects 10 } -- connected users
cmaStatusLicenses OBJECT IDENTIFIER ::= { cmaStatusObjects 30 }
cmaStatusEndpointManagement OBJECT IDENTIFIER ::= { cmaStatusObjects 50 }
cmaStatusDevice OBJECT IDENTIFIER ::= { cmaStatusObjects 60 }
cmaStatusDeviceMCU OBJECT IDENTIFIER ::= { cmaStatusDevice 1 }
cmaStatusDeviceEndpoint OBJECT IDENTIFIER ::= { cmaStatusDevice 2 }
cmaStatusDeviceVBP OBJECT IDENTIFIER ::= { cmaStatusDevice 3 }
cmaStatusDeviceDMA OBJECT IDENTIFIER ::= { cmaStatusDevice 4 }
cmaStatusDevicePeripherals OBJECT IDENTIFIER ::= { cmaStatusDevice 5 }
cmaStatusDeviceSAM OBJECT IDENTIFIER ::= { cmaStatusDevice 6 }
cmaStatusDeviceSBC OBJECT IDENTIFIER ::= { cmaStatusDevice 7 }
cmaStatusConferenceSummary OBJECT IDENTIFIER ::= { cmaStatusObjects 70 }
cmaStatusConferencesOngoing OBJECT IDENTIFIER ::= { cmaStatusObjects 80 }
cmaStatusAlerts OBJECT IDENTIFIER ::= { cmaStatusObjects 90 }
cmaStatusRedundancy OBJECT IDENTIFIER ::= { cmaStatusObjects 100 }
cmaStatusSites OBJECT IDENTIFIER ::= { cmaStatusObjects 110 }
cmaStatusSiteLinks OBJECT IDENTIFIER ::= { cmaStatusObjects 120 }
cmaStatusSubnets OBJECT IDENTIFIER ::= { cmaStatusObjects 130 }

-- SMIv2 Conformance groups

-- Textual Conventions

--NetworkAddress ::= SEQUENCE
--{
--  addressType                InetAddressType,
--  address            InetAddress
--}

CmaDefaultTableIndexRange ::= TEXTUAL-CONVENTION
  DISPLAY-HINT "d"
  STATUS current
  DESCRIPTION "Default table index range."
  SYNTAX Integer32 (1..2147483647)

CmaTimeZone ::= TEXTUAL-CONVENTION
  DISPLAY-HINT "1a1d:1d"
  STATUS current
  DESCRIPTION "A time zone specification.
  field     octets    contents             range
  -----     ------    --------             -----  
  1          1      direction from UTC   '+' / '-'
  2          2      hours from UTC       0..13
  3          3      minutes from UTC     0..59

  Note: Daylight saving time in New Zealand is +13."
  SYNTAX OCTET STRING (SIZE(3))

CmaConfigSystemLogLevel ::= TEXTUAL-CONVENTION
STATUSES current
DESCRIPTION “CMA System log level values.”
SYNTAX INTEGER { debug(0), info(1), warn(2), error(3), fatal(4), off(5) }

CmaConfigLdapSecurityLevel ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION “CMA LDAP security level values.”
SYNTAX INTEGER
{ plain(1),
  startTLS(2),
  ldaps(3)
}

-- CmaConfigDatabaseType ::= TEXTUAL-CONVENTION
-- STATUS current
-- DESCRIPTION “CMA database type values.”
-- SYNTAX INTEGER
--     { internal(1)
--     }

CmaConfigSystemTimeSourceType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION “CMA time source values.”
SYNTAX INTEGER
{ internal(1),
  external(2)
}

CmaConfigRemoteAlertLevel ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION “CMA remote alert level values.”
SYNTAX INTEGER
{ none(0),
  info(1),
  minor(2),
  major(4)
}

-- CmaConfigGatekeeperMessageType ::= TEXTUAL-CONVENTION
-- STATUS current
-- DESCRIPTION “CMA gatekeeper message type values.”
-- SYNTAX INTEGER
--     { rrq(0), ---- Registration Request
--       grq(1), ---- Gatekeeper Request
--       irrIrq(2), ---- Information Response/Information Request
--       lwrrq(3), ---- Light-weight Registration Request
--       urq(4), ---- Unregistration Request
--       lrq(5), ---- Location Request
--       arq(6), ---- Admission Request
--       drq(7), ---- Disengage Request
--       brq(8), ---- Bandwidth Request
--       setup(9), ---- Setup message
--       releaseComplete(10), ---- Non-standard message
--       nsm(11), ---- other(12) ---- other call state changed

---

```plaintext
CmaPrimaryGatekeeperEndpointRegistrationType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "CMA gatekeeper endpoint registration type values."
  SYNTAX INTEGER
  {
    all(1),
    predefinedOnly(2),
    inDefineSites(3),
    predefinedPrefixesOnly(4)
  }

CmaGatekeeperCallModel ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "CMA gatekeeper call model values."
  SYNTAX INTEGER
  {
    directMode(1),
    routedMode(2)
  }

CmaMcuType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "CMA MCU type values."
  SYNTAX INTEGER
  {
    other(0),
    rmx(1),
    mc(2),
    mrc(3)
  }

CmaDeviceStatus ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "CMA device status values."
  SYNTAX INTEGER
  {
    online(1),
    offline(2)
  }

CmaPeripheralPairingStatus ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "CMA device peripheral status values."
  SYNTAX INTEGER
  {
    notPaired(0),
    connected(1),
    disconnected(2),
    unknown(3)
  }

CmaPeripheralIconState ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "CMA peripheral icon status values."
  SYNTAX INTEGER
  {
    noPeripherals(0),
    hasPeripherals(1),
    "...
```

---

```plaintext
```

---

Polycom, Inc. 531
hasPeripheralsWithErrors(2)
}

CmaPeripheralAlertState ::= TEXTUAL-CONVENTION
  current
  DESCRIPTION "CMA peripheral alert status values."
  SYNTAX INTEGER
    { noAlert(0),
      venusSwIncompatible(1)
    }

CmaEndpointType ::= TEXTUAL-CONVENTION
  current
  DESCRIPTION "CMA endpoint type values."
  SYNTAX INTEGER
    { other(0),
      vseries(1),
      vtx1000(6),
      tandberg(7),
      hdx(8),
      cmad(9),
      qdx(10),
      vvx(11),
      lifesize(12),
      venus(13),
      rabbiteye(14),
      rmpmobile(15)
    }

CmaDeviceRegistrationStatus ::= TEXTUAL-CONVENTION
  current
  DESCRIPTION "CMA device registration status values."
  SYNTAX INTEGER
    { unknown(0),
      registered(1),
      notRegistered(2),
      registering(3),
      rejected(4),
      notApplicable(5)
    }

CmaDeviceManagementStatus ::= TEXTUAL-CONVENTION
  current
  DESCRIPTION "CMA endpoint management status values."
  SYNTAX INTEGER
    { unknown(0),
      ok(1),
      notApplicable(2),
      notResponding(3),
      heartbeatTimeout(4),
      signedOut(5),
      credentialsRequired(6),
      credentialsFailed(7),
      behindFirewall(8),
      httpForbidden(9),
    }
rebooting(10)

CmaVbpModel  ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "CMA VBP model values."
SYNTAX        INTEGER
              { unknown(0),
                stSeries(2) }

CmaConferenceType  ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "CMA conference type values."
SYNTAX        INTEGER
              { audioOnly(1),
                video(2) }

CmaConferenceStatus  ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "CMA conference status values."
SYNTAX        INTEGER
              { unknown(0),
                active(1),
                activeAlerts(2),
                future(3), -- for completeness
                futureAlerts(4),
                finished(5), -- for completeness
                deleted(6), -- for completeness
                declined(7) }

CmaSystemAlertType  ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "CMA system alert values."
SYNTAX        INTEGER
              { unknown(0),
                mcuDown(1),
                databaseConnectionDown(2),
                ldapConnectionDown(3),
                cmaFailOver(4),
                licenseCloseToMax(5),
                mcuTimeDiscrepancy(6),
                monitorServiceStopped(7),
                redundantServerOffline(8),
                redundancyConflict(9),
                ldapSysAccountPasswordFailure(10),
                ldapConnectionFailure(11),
                cdrArchiveFail(12),
                versionCausedForceToInternal(13),
                bandwidthUsedSite(14),
                bandwidthUsedSubnet(15),
                bandwidthUsedSiteLink(16),
                auditUsageThresholdExceeded(17),
                alertDiskSpaceUsageExceeded(18),
CmaEndpointAlertType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "CMA endpoint alert values."
SYNTAX INTEGER
{
  remoteControlBatteryLow(0),
  credentialsRequired(1),
  credentialsFailed(2),
  httpForbidden(3),
  notResponding(4),
  heartbeatTimeout(5),
  gatekeeperStatusUnknown(6),
  gatekeeperRejected(7),
  gatekeeperUnregistered(8),
  directoryStatusUnknown(9),
  directoryNotRegistered(10),
  presenceStatusUnknown(11),
  presenceUnregistered(12),
  helpRequest(13),
  mgmtUrlNotSet(14),
  venusDisconnected(15),
  venusSoftwareIncompatible(16),
  sipUriNotProvided(17),
  sipStatusUnknown(18),
  sipUnregistered(19)
}

CmaRedundantServerRole ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "CMA redundant server role values."
SYNTAX INTEGER
{
  primary(1),
  alternate(2)
}

CmaRedundantServerStatus ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "CMA redundant server status values."
SYNTAX INTEGER
{
  online(1),
  offline(2)
SimplifiedDialingEndpointBitRates ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "CMA dial plan service simplified dialing bit rates."
  SYNTAX INTEGER
  {
    notConfigured(0),
    br1B(1),    -- 1B
    br2B(2),    -- 2B
    br3B(3),    -- 3B
    br4B(4),    -- 4B
    br5B(5),    -- 5B
    br6B(6),    -- 6B
    br64(7),    -- 64 kbps
    br128(8),   -- 128 kbps
    br192(9),   -- 192 kbps
    br256(10),  -- 256 kbps
    br320(11),  -- 320 kbps
    br384(12),  -- 384 kbps
    br448(13),  -- 448 kbps
    br512(14),  -- 512 kbps
    br576(15),  -- 576 kbps
    br640(16),  -- 640 kbps
    br704(17),  -- 704 kbps
    br768(18),  -- 768 kbps
    br1152(19), -- 1152 kbps
    br1472(20), -- 1472 kbps
    br1536(21), -- 1536 kbps
    br1920(22)  -- 1920 kbps
  }

MgcVideoSessionType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "MGC video session type."
  SYNTAX INTEGER
  {
    continuousPresence(1),
    switching(2),
    transcoding(3)
  }

ConfOnDemandMgcBitRateType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "MGC bit rate."
  SYNTAX INTEGER
  {
    notConfigured(0),
    br128(1),   -- 128 kbps
    br256(2),   -- 256 kbps
    br384(3),   -- 384 kbps
    br448(4),   -- 448 kbps
    br512(5),   -- 512 kbps
    br576(6),   -- 576 kbps
    br640(7),   -- 640 kbps
    br704(8),   -- 704 kbps
    br768(9),   -- 768 kbps
    br1152(10), -- 1152 kbps
    br1472(11), -- 1472 kbps
    br1536(12), -- 1536 kbps
br1920(13) -- 1920 kbps
}

SiteTopoSiteType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site type."
  SYNTAX INTEGER
  { internetCloud(1), -- Internet
    networkCloud(2), -- MPLS/Network Cloud
    privateSite(3) -- Private/Site
  }

SiteTopoIsdnNumberAssignmentMethodType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology ISDN number assignment method."
  SYNTAX INTEGER
  { none(1),
    did(2),                -- Direct Inward Dial
    gwExtensionDialing(3)  -- Gateway + extension
  }

SiteTopoInternetRoutingType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology internet calling types."
  SYNTAX INTEGER
  { notAllowed(1),           -- call routing through internet not allowed
    viaH323AwareFirewall(2), -- allowed via a H.323 aware firewall
    viaH323SbcOrAlg(3)       -- allowed via a H.323 aware SBC
      -- (Session Border Control) or ALG
      -- (Application level gateway)
  }

SiteProvisioningDateFormatType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology provisioning date format."
  SYNTAX INTEGER
  { monthDayYear(1),   -- MM-dd-yyyy
    dayMonthYear(2),  -- dd-MM-yyyy
    yearMonthDay(3)   -- yyyy-MM-dd
  }

SiteProvisioningTimeFormatType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology provisioning time format."
  SYNTAX INTEGER
  { twelveHour(1),
    twentyFourHour(2)
  }

SiteNatConfigurationType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology provisioning NAT configuration type."
  SYNTAX INTEGER
  { off(1),
auto(2),
  manual(3)
}

SiteUseGkForMultipointCallsType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology provisioning use gatekeeper for multipoint calls setting."
  SYNTAX INTEGER
    { dynamic(1),
      always(2),
      never(3)
    }

SiteTimeServerUpdateType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Time Server would follow time updation in the following ways."
  SYNTAX INTEGER
    { auto(1),
      manual(2),
      off(3) }

SiteQosTypeOfServiceType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology provisioning QOS type."
  SYNTAX INTEGER
    { ipPrecedence(1),
      diffServ(2) }

SiteQosMtuSizeType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology provisioning IP call maximum transmission unit values (bytes)"
  SYNTAX INTEGER
    { ipCallMtu660(1), -- 660
      ipCallMtu780(2), -- 780
      ipCallMtu900(3), -- 900
      ipCallMtu1020(4), -- 1020
      ipCallMtu1140(5), -- 1140
      ipCallMtu1260(6), -- 1260
      ipCallMtu1500(7) -- 1500 }

SiteQosBandwidthType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Site topology provisioning IP call maximum line speed values (Kbps)."
  SYNTAX INTEGER
    { linespeed64(1),
      linespeed128(2),
      linespeed256(3),
      linespeed384(4),
      linespeed512(5),
      linespeed768(6),
      linespeed1024(7),
      linespeed1472(8),
SiteSecurityEnableEncryptionType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Site topology provisioning IP call encryption options."
SYNTAX INTEGER
{
  off(1),                -- No encryption used
  whenAvailable(2),      -- encryption used with any endpoint that supports it.
  requiredForVideo(3),   -- used for all video endpoints in the call, audio & ISDN
                          -- connection are allowed
  requiredForAll(4)      -- used for all video endpoints in the call, audio & ISDN
                          -- connections are not allowed
}

SiteSIPTransportProtocolType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Transport Layer protocol used for SIP."
SYNTAX INTEGER
{
  auto(1),
  tcp(2),
  udp(3),
  tls(4)
}

SiteSIPServerType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Server used for SIP."
SYNTAX INTEGER
{
  standard(1),
  polycom(2),
  microsoft(3),
  siemens(4),
  broadsoft(5),
  avaya(6),
  cisco(7)
}

ConferenceTemplateVideoDialType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference template video dial options."
SYNTAX INTEGER
{
  dialinOnly(1),        -- dial-in only
  dialoutOnly(2),       -- dial-out only
  dialinDialout(3)      -- dial-in and dial-out
}

ConferenceTemplateVideoMode ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference template video layout modes."
SYNTAX INTEGER
{  
  videoSwitching(1),
  oneByOne(2),
  oneByTwo(3),
  twoByOne(4),
  oneByTwoVertical(5),
  oneByTwoHorizontal(6),
  oneByTwoHorizontalUpper(7),
  oneAndTwoHorizontal(8),
  oneAndTwoVertical(9),
  twoByTwo(10),
  oneAndThreeHorizontalUpper(11),
  oneAndThreeHorizontal(12),
  oneAndThreeVertical(13),
  oneAndFourHorizontalUpper(14),
  oneAndFourHorizontal(15),
  oneAndFourVertical(16),
  oneAndFive(17),
  oneAndSeven(18),
  threeByThree(19),
  oneAndEightLower(20),
  oneAndEightUpper(21),
  oneAndEightCentral(22),
  fourByFour(23),
  twoAndEight(24),
  oneAndTwelve(25)
}

ConferenceTemplateVideoAlgorithm ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference template video compression algorithm types."
SYNTAX INTEGER
{  
  auto(1),
  h261(2),
  h263(3),
  h264(4)
}

ConferenceTemplateContentType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference template people and content format types."
SYNTAX INTEGER
{  
  none(1),
  peopleAndContent(2),
  peopleAndContentV0(3),
  polycomVisualConcertPc(4),
  polycomVisualConcertFx(5),
  duoVideo(6)
}

ConferenceTemplateConferenceSpeed ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference template conference speeds (Kbps)."
SYNTAX INTEGER
{  
  confSpeed128(1),
  confSpeed256(2),
  confSpeed320(3),
  confSpeed480(4),
  confSpeed640(5),
  confSpeed960(6),
  confSpeed1280(7)
}
ConferenceTemplateVideoQualityType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference video quality type."
SYNTAX INTEGER
{ motion(1),
  sharpness(2) }

ConferenceTemplateT120Rates ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference T.120 transfer rate."
SYNTAX INTEGER
{ none(1), -- T.120 is not enabled
  m1p6dot4(2), -- MLP 6.4K
  m1p14dot4(3), -- MLP 14.4K
  m1p16(4), -- MLP 16K
  m1p22dot4(5), -- MLP 22.4K
  m1p24(6), -- MLP 24K
  m1p30dot4(7), -- MLP 30.4K
  m1p32(8), -- MLP 32K
  m1p38dot4(9), -- MLP 38.4
  m1p40(10), -- MLP 40K
  m1p46dot4(11), -- MLP 46.4K
  hm1p14dot4(12), -- HMLP 14.4K
  hm1p62dot4(13) -- HMLP 62.4K }

ConferenceTemplateAudioAlgorithms ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference audio compression algorithm used on the MGC MCU."
SYNTAX INTEGER
{ auto(1),
  siren7b16(2),
  siren14b24(3),
  siren14b32(4),
  siren14b48(5),
  g722b56(6),
  g711b56(7) }

ConferenceTemplateLectureModeType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "Conference template lecture mode values."
SYNTAX INTEGER
ConferenceTemplateHDResolution ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Conference template high definition resolution values."
  SYNTAX INTEGER
  {
    sd(1),
    hd720p30(2),
    hd720p60(3),
    hd1080(4)
  }

ConferenceTemplateLastQuitType ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Conference template auto terminate quit type."
  SYNTAX INTEGER
  {
    afterLastQuit(1),
    whenLastRemain(2)
  }

ConferenceTemplateTelepresenceMode ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Conference template telepresence mode."
  SYNTAX INTEGER
  {
    auto(1),
    on(2),
    off(3)
  }

ConferenceTemplateTelepresenceLayoutMode ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Conference template telepresence layout mode."
  SYNTAX INTEGER
  {
    manual(1),
    cp(2),
    roomSwitch(3)
  }

ConferenceTemplateMaxResolution ::= TEXTUAL-CONVENTION
  STATUS current
  DESCRIPTION "Conference template maximum resolution."
  SYNTAX INTEGER
  {
    auto(1),
    cif(2),
    sd(3),
    hd720(4),
    hd1080(5)
  }

ConferenceTemplateContentMode ::= TEXTUAL-CONVENTION
  STATUS current
DESCRIPTION   "Conference template content mode."
SYNTAX        INTEGER
             {  
                 graphics(1),
                 hiResGraphics(2),
                 liveVideo(3)
             }

ConferenceTemplateContentProtocol ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "Conference template content protocol."
SYNTAX        INTEGER
             {  
                 h263(1),
                 upToH264(2)
             }

ConferenceTemplateDisplayLanguage ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "Conference template gathering display language."
SYNTAX        INTEGER
             {  
                 english(1),
                 german(2),
                 spanishSouthAmerica(3),
                 french(4),
                 japanese(5),
                 korean(6),
                 chineseSimplified(7)
             }

ConferenceTemplateRecordingPolicy ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "Conference template recording policy."
SYNTAX        INTEGER
             {  
                 immediately(1),
                 uponRequest(2)
             }

ConferenceTemplateSkin ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "Conference template skin."
SYNTAX        INTEGER
             {  
                 cleanSlate(1),
                 simplyBlue(2),
                 sapphireJewel(3),
                 loopy(4)
             }

UserRoleSchedulingLevel ::= TEXTUAL-CONVENTION
STATUS        current
DESCRIPTION   "User role scheduling levels."
SYNTAX        INTEGER
             {  
                 basic(1),
                 advanced(2),
                 view-only(3)
             }
UserGroupType ::= TEXTUAL-CONVENTION
STATUS   current
DESCRIPTION   "User group type."
SYNTAX     INTEGER
             { local(1),
             enterprise(2) }

RedundancyStatusType ::= TEXTUAL-CONVENTION
STATUS   current
DESCRIPTION   "CMA redundancy status."
SYNTAX     INTEGER
             { notConfigured(1),
             configured(2),           -- configured and okay
             errorNeedsVirtualIp(3),  -- needs virtual IP
             errorSecondaryDown(4)    -- secondary CMA server is down
             }

SnmpVersionType ::= TEXTUAL-CONVENTION
STATUS   current
DESCRIPTION   "CMA SNMP version."
SYNTAX     INTEGER
             { disabled(1),
             v2c(2),
             v3Usm(3)     -- V3 User Based Security Model
             }

SnmpTransportType ::= TEXTUAL-CONVENTION
STATUS   current
DESCRIPTION   "CMA SNMP transport type."
SYNTAX     INTEGER
             { tcp(1),
             udp(2) }

SnmpAuthenticationType ::= TEXTUAL-CONVENTION
STATUS   current
DESCRIPTION   "CMA SNMP authentication type."
SYNTAX     INTEGER
             { sha(1),
             md5(2),
             none(3) }

SnmpEncryptionType ::= TEXTUAL-CONVENTION
STATUS   current
DESCRIPTION   "CMA SNMP encryption type."
SYNTAX     INTEGER
             { des(1),
             aes128bit(2),
             none(3) }

SnmpNotificationType ::= TEXTUAL-CONVENTION
STATUS   current
DESCRIPTION "CMA SNMP notification type."
SYNTAX INTEGER
{
    trap(1),
    inform(2)
}

CmaConfigDayOfWeek ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION ""
SYNTAX INTEGER
{
    undefined(0),
    sunday(1),
    monday(2),
    tuesday(3),
    wednesday(4),
    thursday(5),
    friday(6),
    saturday(7)
}

-- Configuration Group

-- START general configuration

cmaConfigGeneralGroup OBJECT-GROUP
OBJECTS
{
    cmaConfigSoftwareVersion,
    cmaConfigCMADSoftwareVersion,
    cmaConfigRemoteAccessEnabled,
    cmaConfigCMADMacSoftwareVersion,
    cmaConfigCMADShippedSoftwareVersion,
    cmaConfigCMADMacShippedSoftwareVersion,
    cmaConfigHardwareVersion
}
STATUS current
DESCRIPTION "CMA general configuration group."
::= { cmaConfigConformance 1 }

cmaConfigSoftwareVersion OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA software version."
::= { cmaConfigGeneral 1 }

cmaConfigCMADSoftwareVersion OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Software version of the downloadable CMADesktop client."
::= { cmaConfigGeneral 2 }

cmaConfigRemoteAccessEnabled OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
MIB Reference

STATUS current
DESCRIPTION "Remote access enabled flag"
::= { cmaConfigGeneral 3 }

cmaConfigOMADMacSoftwareVersion OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Software version of the downloadable CMADesktop Mac client."
::= { cmaConfigGeneral 4 }

cmaConfigOMADShippedSoftwareVersion OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Software version of the shipped CMADesktop client."
::= { cmaConfigGeneral 5 }

cmaConfigOMADMacShippedSoftwareVersion OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Software version of the shipped CMADesktop Mac client."
::= { cmaConfigGeneral 6 }

cmaConfigHardwareVersion OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA Hardware Version."
::= { cmaConfigGeneral 7 }

-- END general configuration

-- START Admin contact configuration

cmaConfigAdminContactGroup OBJECT-GROUP
OBJECTS
{
  cmaConfigAdminContactName,
  cmaConfigAdminContactEmailAddress,
  cmaConfigAdminContactTitle,
  cmaConfigAdminContactDepartment,
  cmaConfigAdminContactCity,
  cmaConfigAdminContactPhoneNumber
}
STATUS current
DESCRIPTION "CMA administrator contact configuration group."
::= { cmaConfigConformance 2 }

cmaConfigAdminContactName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA administrator contact name."
::= { cmaConfigContact 1 }

cmaConfigAdminContactEmailAddress OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
cmaConfigAdminContactTitle OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA administrator title."
 ::= { cmaConfigContact 3 }

cmaConfigAdminContactDepartment OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA administrator department."
 ::= { cmaConfigContact 4 }

cmaConfigAdminContactCity OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA administrator city."
 ::= { cmaConfigContact 5 }

cmaConfigAdminContactPhoneNumber OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA administrator phone number."
 ::= { cmaConfigContact 6 }

-- END Admin contact configuration

-- START Log configuration

cmaConfigLogGroup OBJECT-GROUP
OBJECTS
{
   cmaConfigSystemLogLevel
   --> cmaConfigGatekeeperLogMessageType, 
   --> cmaConfigGatekeeperLogMessageEnabled

   STATUS current
   DESCRIPTION "CMA log configuration group."
   ::= { cmaConfigConformance 3 }

   -- CmaConfigGatekeeperLogSettingEntry ::= SEQUENCE
   -- {
   --   cmaConfigGatekeeperLogMessageType CmaConfigGatekeeperMessageType,
   --   cmaConfigGatekeeperLogMessageEnabled TruthValue
   -- } 

   cmaConfigSystemLogLevel OBJECT-TYPE
   SYNTAX CmaConfigSystemLogLevel
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION "CMA system log level setting."
   ::= { cmaConfigLog 1 }
-- cmaConfigGatekeeperLogSettingTable OBJECT-TYPE
-- SYNTAX        SEQUENCE OF CmaConfigGatekeeperLogSettingEntry
-- MAX-ACCESS    not-accessible
-- STATUS        current
-- DESCRIPTION   "CMA gatekeeper log setting table. Contains log setting
-- information for each gatekeeper message type.”
-- ::= { cmaConfigLog 2 }

-- cmaConfigGatekeeperLogSettingEntry OBJECT-TYPE
-- SYNTAX        CmaConfigGatekeeperLogSettingEntry
-- MAX-ACCESS    not-accessible
-- STATUS        current
-- DESCRIPTION   "CMA gatekeeper log setting entry.”
-- INDEX         { cmaConfigGatekeeperLogMessageType }
-- ::= { cmaConfigGatekeeperLogSettingTable 1 }

-- cmaConfigGatekeeperLogMessageType OBJECT-TYPE
-- SYNTAX        CmaConfigGatekeeperMessageType
-- MAX-ACCESS    read-only
-- STATUS        current
-- DESCRIPTION   "Message type of the gatekeeper log setting entry.”
-- ::= { cmaConfigGatekeeperLogSettingEntry 2 }

-- cmaConfigGatekeeperLogMessageEnabled OBJECT-TYPE
-- SYNTAX        TruthValue
-- MAX-ACCESS    read-only
-- STATUS        current
-- DESCRIPTION   "Flag indicating whether this message type is logged.”
-- ::= { cmaConfigGatekeeperLogSettingEntry 3 }

-- END Log contact configuration

-- START LDAP configuration

cmaConfigLdapGroup OBJECT-GROUP
OBJECTS
{ cmaConfigLdapEnabled,
  cmaConfigLdapServerInetAddressType,
  cmaConfigLdapServerInetAddress,
  cmaConfigLdapSecurityLevel,
  cmaConfigLdapIgnoreDisabledADUsers,
  cmaConfigLdapExclusionFilter,
  cmaConfigLdapSearchBaseDN,
  cmaConfigLdapWindowsAuthenticationIntegration,
  cmaConfigLdapWindowsAuthenticationDomainControllerName
}
STATUS current
DESCRIPTION "CMA LDAP configuration conformance group.”
 ::= { cmaConfigConformance 4 }

cmaConfigLdapEnabled OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "LDAP integration enabled flag.”
 ::= { cmaConfigLDAP 1 }

cmaConfigLdapServerInetAddressType OBJECT-TYPE
SYNTAX     InetAddressType
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "IP address type of the LDAP server."
::= { cmaConfigLDAP 2 }

cmaConfigLdapServerInetAddress  OBJECT-TYPE
SYNTAX     InetAddress
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "IP address or DNS name of the LDAP server."
::= { cmaConfigLDAP 3 }

cmaConfigLdapSecurityLevel  OBJECT-TYPE
SYNTAX     CmaConfigLdapSecurityLevel
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "LDAP security level."
::= { cmaConfigLDAP 4 }

cmaConfigLdapIgnoreDisabledADUsers  OBJECT-TYPE
SYNTAX     TruthValue
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Flag indicating whether to ignore disabled active directory users."
::= { cmaConfigLDAP 5 }

cmaConfigLdapExclusionFilter  OBJECT-TYPE
SYNTAX     OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "LDAP exclusion filter."
::= { cmaConfigLDAP 6 }

cmaConfigLdapSearchBaseDN  OBJECT-TYPE
SYNTAX     OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "LDAP search base distinguished name."
::= { cmaConfigLDAP 7 }

cmaConfigLdapWindowsAuthenticationIntegration  OBJECT-TYPE
SYNTAX     TruthValue
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Windows Authentication integration flag."
::= { cmaConfigLDAP 8 }

cmaConfigLdapWindowsAuthenticationDomainControllerName  OBJECT-TYPE
SYNTAX     OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Windows domain controller name."
::= { cmaConfigLDAP 9 }

-- END LDAP contact configuration

-- START database configuration
-- cmaConfigDatabaseGroup OBJECT-GROUP
-- OBJECTS
-- {
--    cmaConfigDatabaseType,
--    cmaConfigExternalDatabaseInetAddressType,
--    cmaConfigExternalDatabaseInetAddress,
--    cmaConfigExternalDatabasePort
-- }
-- STATUS current
-- DESCRIPTION "CMA database configuration conformance group."
-- ::= { cmaConfigConformance 5 }

-- cmaConfigDatabaseType OBJECT-TYPE
-- SYNTAX        CmaConfigDatabaseType
-- MAX-ACCESS    read-only
-- STATUS        current
-- DESCRIPTION   "CMA database type (internal or external)."
-- ::= { cmaConfigDatabase 1 }

-- cmaConfigExternalDatabaseInetAddressType OBJECT-TYPE
-- SYNTAX        InetAddressType
-- MAX-ACCESS    read-only
-- STATUS        current
-- DESCRIPTION   "IP address type of external database (only valid
-- if external database is being used)."
-- ::= { cmaConfigDatabase 2 }

-- cmaConfigExternalDatabaseInetAddress OBJECT-TYPE
-- SYNTAX        InetAddress
-- MAX-ACCESS    read-only
-- STATUS        current
-- DESCRIPTION   "IP address of external database (only valid if
-- external database is being used)."
-- ::= { cmaConfigDatabase 3 }

-- cmaConfigExternalDatabasePort OBJECT-TYPE
-- SYNTAX        InetPortNumber
-- MAX-ACCESS    read-only
-- STATUS        current
-- DESCRIPTION   "IP port of external database (only valid if external
-- database is being used)."
-- ::= { cmaConfigDatabase 4 }

-- END database configuration

-- START system time configuration

cmaConfigSystemTimeGroup OBJECT-GROUP
OBJECTS
{
    cmaConfigSystemTimeZone,
    cmaConfigSystemTimeDaylightSavingAutoAdjust,
    cmaConfigSystemTimeSourceType,
    -- cmaConfigSystemTimeExternalSourceSyncPeriod,
    timeSourceIndex,
    timeSourceInetAddressType,
    timeSourceInetAddress
}
STATUS current
DESCRIPTION "CMA System time configuration conformance group."
::= { cmaConfigConformance 6 }

cmaConfigSystemTimeZone OBJECT-TYPE
SYNTAX        CmaTimeZone
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Time zone in which the CMA server resides.”
::= { cmaConfigTime 1 }

cmaConfigSystemTimeDaylightSavingAutoAdjust OBJECT-TYPE
SYNTAX        TruthValue
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Daylight saving auto adjust flag.”
::= { cmaConfigTime 2 }

cmaConfigSystemTimeSourceType OBJECT-TYPE
SYNTAX        CmaConfigSystemTimeSourceType
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Time source type.”
::= { cmaConfigTime 3 }

-- cmaConfigSystemTimeExternalSourceSyncPeriod OBJECT-TYPE
-- SYNTAX      Integer32
-- MAX-ACCESS  read-only
-- STATUS      current
-- DESCRIPTION “Number of minutes between synchronization attempts with external
--               time source (only valid if external time source is used).”
-- ::= { cmaConfigTime 4 }

CmaConfigSystemTimeExternalSourceTableEntry ::= SEQUENCE
{ timeSourceIndex               CmaDefaultTableIndexRange,
timeSourceInetAddressType     InetAddressType,
timeSourceInetAddress         InetAddress
}

cmaConfigSystemTimeExternalSourceTable OBJECT-TYPE
SYNTAX        SEQUENCE OF CmaConfigSystemTimeExternalSourceTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   “External time source table. Contains time server addresses.”
::= { cmaConfigSystemTimeExternalSourceTable 1 }

cmaConfigSystemTimeExternalSourceEntry OBJECT-TYPE
SYNTAX        CmaConfigSystemTimeExternalSourceTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   “External time source table entry.”
INDEX         { timeSourceIndex }
::= { cmaConfigSystemTimeExternalSourceEntry 1 }

timeSourceIndex OBJECT-TYPE
SYNTAX      CmaDefaultTableIndexRange
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Unique system-assigned ID for this entry.”
::= { cmaConfigSystemTimeExternalSourceEntry 1 }
timeSourceInetAddressType OBJECT-TYPE
SYNTAX    InetAddressType
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "IP address type of the external time source."
 ::= { cmaConfigSystemTimeExternalSourceEntry 2 }

timeSourceInetAddress OBJECT-TYPE
SYNTAX    InetAddress
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "IP address or DNS name of the external time source."
 ::= { cmaConfigSystemTimeExternalSourceEntry 3 }

-- END system time configuration

-- START Redundancy settings

CMAConfigRedundancyGroup OBJECT-GROUP
OBJECTS
{  
  CMAConfigRedundancyEnabled,
  CMAConfigRedundancyVirtualInetAddressType,
  CMAConfigRedundancyVirtualInetAddress
}
STATUS current
DESCRIPTION "CMA redundancy configuration conformance group."
 ::= { CMAConfigConformance 7 }

CMAConfigRedundancyEnabled OBJECT-TYPE
SYNTAX    TruthValue
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Redundancy enabled flag."
 ::= { CMAConfigRedundancy 1 }

CMAConfigRedundancyVirtualInetAddressType OBJECT-TYPE
SYNTAX    InetAddressType
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "IP address type of the virtual IP (valid only if redundancy is enabled)."
 ::= { CMAConfigRedundancy 2 }

CMAConfigRedundancyVirtualInetAddress OBJECT-TYPE
SYNTAX    InetAddress
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "IP address of the virtual IP (valid only if redundancy is enabled)."
 ::= { CMAConfigRedundancy 3 }

-- END Redundancy settings

-- START Remote Alert Settings

CMAConfigRemoteAlertGroup OBJECT-GROUP
OBJECTS
{  

cmaConfigRemoteAlertsEnabled,
cmaConfigRemoteStartupQuiescentTime,
cmaConfigSystemAlertType,
cmaConfigSystemAlertLevel,
cmaConfigEndpointAlertType,
cmaConfigEndpointAlertLevel
}

STATUS current
DESCRIPTION “CMA remote alert configuration conformance group.”
::= { cmaConfigConformance 8 }

cmaConfigRemoteAlertsEnabled OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Remote alerts enabled flag.”
::= { cmaConfigRemoteAlert 1 }

cmaConfigRemoteStartupQuiescentTime OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Number of minutes after a startup of CMA before remote alerts are sent
(only valid if remote alerts are enabled). This period of time allows the
CMA server to finish startup activities. Only alerts that are still
outstanding at the end of the period are sent.”
::= { cmaConfigRemoteAlert 2 }

CmaConfigSystemAlertSettingEntry ::= SEQUENCE
{
cmaConfigSystemAlertType CmaSystemAlertType,
cmaConfigSystemAlertLevel CmaConfigRemoteAlertLevel
}

CmaConfigSystemAlertSettingTable OBJECT-TYPE
SYNTAX SEQUENCE OF CmaConfigSystemAlertSettingEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION “System alert level settings table. Contains system alert types
and their alert levels.”
::= { cmaConfigRemoteAlert 3 }

CmaConfigSystemAlertSettingEntry OBJECT-TYPE
SYNTAX CmaConfigSystemAlertSettingEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION “System alert level settings table entry.”
INDEX { cmaConfigSystemAlertType }
::= { cmaConfigSystemAlertSettingTable 1 }

CmaConfigSystemAlertType OBJECT-TYPE
SYNTAX CmaSystemAlertType
MAX-ACCESS read-only
STATUS current
DESCRIPTION “System alert type.”
::= { cmaConfigSystemAlertSettingEntry 1 }

CmaConfigSystemAlertLevel OBJECT-TYPE
SYNTAX CmaConfigRemoteAlertLevel
MAX-ACCESS read-only
MIB Reference

Polycom, Inc. 553

STATUS current
DESCRIPTION "Alert level of the system alert type."
 ::= { cmaConfigSystemAlertSettingEntry 2 }

CmaConfigEndpointAlertSettingEntry ::= SEQUENCE
{
    cmaConfigEndpointAlertType CmaEndpointAlertType,
cmaConfigEndpointAlertLevel CmaConfigRemoteAlertLevel
}

CmaConfigEndpointAlertSettingTable OBJECT-TYPE
SYNTAX SEQUENCE OF CmaConfigEndpointAlertSettingEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "Endpoint alert level settings table. Contains endpoint alert types and their alert levels."
 ::= { cmaConfigRemoteAlert 4 }

CmaConfigEndpointAlertSettingEntry OBJECT-TYPE
SYNTAX CmaConfigEndpointAlertSettingEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "Endpoint alert level settings table entry."
INDEX { cmaConfigEndpointAlertType }
 ::= { cmaConfigEndpointAlertSettingTable 1 }

CmaConfigEndpointAlertType OBJECT-TYPE
SYNTAX CmaEndpointAlertType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Endpoint alert type."
 ::= { cmaConfigEndpointAlertSettingEntry 1 }

CmaConfigEndpointAlertLevel OBJECT-TYPE
SYNTAX CmaConfigRemoteAlertLevel
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Alert level of the endpoint alert type."
 ::= { cmaConfigEndpointAlertSettingEntry 2 }

-- END Remote Alert Settings

-- START Network settings

cmaConfigNetworkGroup OBJECT-GROUP
OBJECTS
{
    cmaConfigNetworkSystemName,
cmaConfigNetworkInetAddressType,
cmaConfigNetworkInetAddress,
cmaConfigNetworkSubnetMask,
cmaConfigNetworkDefaultGatewayInetAddressType,
cmaConfigNetworkDefaultGatewayInetAddress,
cmaConfigNetworkPreferedDnsServerInetAddressType,
cmaConfigNetworkPreferedDnsServerInetAddress,
cmaConfigNetworkAlternateDnsServerInetAddressType,
cmaConfigNetworkAlternateDnsServerInetAddress,
cmaConfigNetworkDnsServerDomain
}

Polycom, Inc. 553
STATUS current
DESCRIPTION "CMA Network configuration conformance group."
::= { cmaConfigConformance 10 }

cmaConfigNetworkSystemName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA server’s system name."
::= { cmaConfigNetwork 1 }

cmaConfigNetworkInetAddressType OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA server’s IP address type."
::= { cmaConfigNetwork 2 }

cmaConfigNetworkInetAddress OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA server’s IP address."
::= { cmaConfigNetwork 3 }

cmaConfigNetworkSubnetMask OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA server’s subnet mask."
::= { cmaConfigNetwork 4 }

cmaConfigNetworkDefaultGatewayInetAddressType OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Default gateway IP address type."
::= { cmaConfigNetwork 5 }

cmaConfigNetworkDefaultGatewayInetAddress OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Default gateway IP address."
::= { cmaConfigNetwork 6 }

cmaConfigNetworkPreferredDnsServerInetAddressType OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Preferred DNS server IP address type."
::= { cmaConfigNetwork 7 }

cmaConfigNetworkPreferredDnsServerInetAddress OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Preferred DNS server IP address."
::= { cmaConfigNetwork 8 }
cmaConfigNetworkAlternateDnsServerInetAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Alternate DNS server IP address type."
::= { cmaConfigNetwork 9 }

cmaConfigNetworkAlternateDnsServerInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Alternate DNS server IP address."
::= { cmaConfigNetwork 10 }

cmaConfigNetworkDnsServerDomain OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "DNS server domain name."
::= { cmaConfigNetwork 11 }

-- END Network settings

-- START email settings

cmaConfigEmailGroup OBJECT-GROUP
OBJECTS
{ cmaConfigEmailCount, emailConfigIndex, cmaConfigEmailFromAddress, cmaConfigEmailSmtpServerInetAddressType, cmaConfigEmailSmtpServerInetAddress }
STATUS current
DESCRIPTION "CMA email configuration conformance group."
::= { cmaConfigConformance 11 }

cmaConfigEmailCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of email configurations."
::= { cmaConfigEmail 1 }

EmailConfigTableEntry ::= SEQUENCE
{ emailConfigIndex CmaDefaultTableIndexRange, cmaConfigEmailFromAddress OCTET STRING, cmaConfigEmailSmtpServerInetAddressType InetAddressType, cmaConfigEmailSmtpServerInetAddress InetAddress }

cmaConfigEmailTable OBJECT-TYPE
SYNTAX SEQUENCE OF EmailConfigTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "Email configuration table."
::= { cmaConfigEmail 2 }
emailConfigTableEntry OBJECT-TYPE
  SYNTAX        EmailConfigTableEntry
  MAX-ACCESS    not-accessible
  STATUS        current
  DESCRIPTION   “Email config entry.”
  INDEX         { emailConfigIndex }
  ::= { cmaConfigEmailTable 1 }

emailConfigIndex OBJECT-TYPE
  SYNTAX        CmaDefaultTableIndexRange
  MAX-ACCESS    read-only
  STATUS        current
  DESCRIPTION   “Unique system-assigned ID for this entry.”
  ::= { emailConfigTableEntry 1 }

cmaConfigEmailFromAddress  OBJECT-TYPE
  SYNTAX        OCTET STRING (SIZE(0..255))
  MAX-ACCESS    read-only
  STATUS        current
  DESCRIPTION   “CMA server’s email ‘From’ address.”
  ::= { emailConfigTableEntry 2 }

cmaConfigEmailSmtpServerInetAddressType  OBJECT-TYPE
  SYNTAX        InetAddressType
  MAX-ACCESS    read-only
  STATUS        current
  DESCRIPTION   “IP address type of the SMTP server.”
  ::= { emailConfigTableEntry 3 }

cmaConfigEmailSmtpServerInetAddress  OBJECT-TYPE
  SYNTAX        InetAddress
  MAX-ACCESS    read-only
  STATUS        current
  DESCRIPTION   “IP address of the SMTP server.”
  ::= { emailConfigTableEntry 4 }

-- END email settings

-- START UI Settings

cmaConfigUIGroup  OBJECT-GROUP
  OBJECTS
  {
    cmaConfigUIDefaultProfileAccessAllowed,
    cmaConfigUIMaxSessionPerUser
  }
  STATUS        current
  DESCRIPTION   “CMA UI configuration conformance group.”
  ::= { cmaConfigConformance 12 }

cmaConfigUIDefaultProfileAccessAllowed OBJECT-TYPE
  SYNTAX        TruthValue
  MAX-ACCESS    read-only
  STATUS        current
  DESCRIPTION   “Flag indicating whether users without explicit roles are allowed to log into
                 the CMA UI and are assigned the default profile.”
  ::= { cmaConfigUI 1 }

cmaConfigUIMaxSessionPerUser OBJECT-TYPE
  SYNTAX        Integer32
  MAX-ACCESS    read-only
STATUS current
DESCRIPTION "The Maximum Number of Sessions allowed per user. The default and minimum value is 1. It returns a 0 if disabled."
::= { cmaConfigUI 2 }

-- END UI Settings

-- START endpoint management settings
cmaConfigEndpointGroup OBJECT-GROUP
OBJECTS
{
cmaConfigEndpointAutoDiscovery,
cmaConfigEndpointUseCommonPassword
}
STATUS current
DESCRIPTION "CMA Endpoint management configuration conformance group."
::= { cmaConfigConformance 13 }
cmaConfigEndpointAutoDiscovery OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether automatic endpoint discovery is enabled."
::= { cmaConfigEndpoint 1 }
cmaConfigEndpointUseCommonPassword OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether a common administrator password is used for all endpoints."
::= { cmaConfigEndpoint 2 }

-- END endpoint management settings

-- START Dial Plans - dial rules
cmaConfigSiteGroup OBJECT-GROUP
OBJECTS
{
sitetopologySiteProvisioningCount,
siteProvisioningSiteName,
siteCountry,
siteDateFormat,
siteAutoAdjustDst,
siteTimeFormat,
siteTimeServerUpdateType,
sitePrimaryTimeServerInetAddressType,
sitePrimaryTimeServerInetAddress,
siteSecondaryTimeServerInetAddressType,
siteSecondaryTimeServerInetAddress,
siteTimeZone,
siteFirewallUseFixedPorts,
siteFirewallTcpStartPort,
siteFirewallUdpStartPort,
siteFirewallH460Traversal,
siteFirewallNatConfiguration,
siteFirewallNatWanAddressType,
siteFirewallNatWanAddress,
siteFirewallNatH323Compatible,
siteFirewallShowEpInGab,
siteFirewallEnableSipKeepAlives,
siteH323EnableIpCalls,
siteH323GatekeeperIPAddressType,
siteH323GatekeeperIPAddress,
siteH323UseGkForMultipointCalls,
siteProvisioningPollingInterval,
siteSoftupdatePollingInterval,
siteQosVideoTosValue,
siteQosAudioTosValue,
siteQosFeccTosValue,
siteQosToType,
siteQosMaxMtuSize,
siteQosEnablePvec,
siteQosEnableRsvp,
siteQosDynamicBandwidth,
siteQosMaxTransmitBandwidth,
siteQosMaxReceiveBandwidth,
siteSecurityUsePwdForRemoteAccess,
siteSecurityEnableSecureMode,
siteSecurityEnableEncryption,
siteSecurityEnableWebAccess,
siteSecurityEnableTelnetAccess,
siteSecurityEnableSnmpAccess,
siteSecurityWebAccessPort,
siteSecurityAllowWebVideoDisplay,
siteSecurityMtlnVersion,
siteCmadHeartbeatPollingInterval,
siteCmadInCallStatsPollingInterval,
siteCalendaringExchangeServerIPAddressType,
siteCalendaringExchangeServerIPAddress,
siteSIPEnable,
siteSIPDomain,
siteSIPAutoDiscoverServer,
siteSIPProxyServerInetAddressType,
siteSIPProxyServerInetAddress,
siteSIPRegistrarServerInetAddressType,
siteSIPRegistrarServerInetAddress,
siteSIPBackupProxyServerInetAddressType,
siteSIPBackupProxyServerInetAddress,
siteSIPBackupRegistrarServerInetAddressType,
siteSIPBackupRegistrarServerInetAddress,
siteSIPTransportLayerProtocol,
siteSIPServerType,
siteSIPVerifyCertificate,
siteSIPUseEnterpriseCredentials,
siteSecurityProfile,
siteSecurityIdleSessionTimeout,
siteSecurityFailedLoginThreshold,
siteSecurityFailedLoginWindow,
siteSecurityPortLockoutDuration,
siteSecurityMaxCertificateVerificationDepth,
siteSecurityVerifyCertforWebAccess,
--
siteEnableEnterpriseDir,
siteEnterpriseDirAdminGroup,
siteEnterpriseDirUserGroup,
siteDirectorySettingsUseThisServer,
siteDirectorySettingsServerIPAddress,
siteDirectorySettingsVerifyCertificate,
sitePresenceSettingsUseThisServer,
MIB Reference

Polycom, Inc. 559

sitePresenceSettingsServerIPAddress,
sitePresenceSettingsVerifyCertificate,
sitetoPOlogySAMSiteProvisioningCount,
samsiteProvisioningSiteName,
samsiteTimeServerUpdateType,
samsitePrimaryTimeServerInetAddressType,
samsitePrimaryTimeServerInetAddress,
samsiteSecondaryTimeServerInetAddressType,
samsiteSecondaryTimeServerInetAddress,
samsiteProvisioningPollingInterval,
samsiteCmdHeartbeatPollingInterval,
samsiteServerStatusPollingInterval,
samsiteH323EnableIpCalls,
samsiteH323GatekeeperIPAddressType,
samsiteH323GatekeeperIPAddress,
samsiteSIPEnable,
samsiteSIPProxyServerInetAddressType,
samsiteSIPProxyServerInetAddress,
samsiteSIPRegistrarServerInetAddressType,
samsiteSIPRegistrarServerInetAddress,
samsiteSIPTransportLayerProtocol,
samsiteSIPVerifyCertificate,
samsiteDirectorySettingsUseThisServer,
samsiteDirectorySettingsServerIPAddress,
samsiteDirectorySettingsVerifyCertificate,
samsitePresenceSettingsUseThisServer,
samsitePresenceSettingsServerIPAddress,
samsitePresenceSettingsVerifyCertificate

}::= { cmaConfigConformance 14 }

-- START Site Topology

cmaConfigSiteTopologyGroup OBJECT-GROUP
OBJECTS
{
siteTopoSiteCount,
siteIndex,
siteName,
siteDescription,
siteOverrideItuDialingRules,
sitePbxAccessCode,
siteCountryCode,
siteAreaCode,
siteNumSubscriberDigits,
siteIsdnNumberAssignmentMethod,
siteInternetRoutingType,
siteSendDialStringtoSBCorALG,
siteCallSignallingInetAddressType,
siteCallSignallingInetAddress,
siteSubnetCount,
siteIsdnGatewayPhoneNumber,
siteIsdnE164Start,
siteIsdnE164End,
siteIsdnCl1Digits,
siteIsdnShortPhoneNumber,
siteIsdnNumberRangeList,
status current
description "CMA Site topology configuration conformance group."
::= { cmaConfigConformance 15 }

-- Sites

siteTopoSiteCount OBJECT-TYPE
  SYNTAX      Integer32
  MAX-ACCESS  read-only
  STATUS      current
  description "Number of configured sites."
  ::= { cmaConfigSiteTopology 1 }

SiteTopoSiteTableEntry ::= SEQUENCE


{  
  siteIndex CmaDefaultTableIndexRange,  
  siteName OCTET STRING,  
  siteDescription OCTET STRING,  
  siteOverrideItuDialingRules TruthValue,  
  sitePbxAccessCode OCTET STRING,  
  siteCountryCode OCTET STRING,  
  siteAreaCode OCTET STRING,  
  siteNumSubscriberDigits Integer32,  
  siteIsdnNumberAssignmentMethod SiteTopoIsdnNumberAssignmentMethodType,  
  siteInternetRoutingType SiteTopoInternetRoutingType,  
  siteSendDialStringtoSBCorALG TruthValue,  
  siteCallSignallingInetAddressType InetAddressType,  
  siteCallSignallingInetAddress InetAddress,  
  siteSubnetCount Integer32,  
  siteIsdnGatewayPhoneNumber OCTET STRING,  
  siteIsdnE164Start OCTET STRING,  
  siteIsdnE164End OCTET STRING,  
  siteIsdnClidigits Integer32,  
  siteIsdnShortPhoneDigits Integer32,  
  siteIsdnNumberRangeList OCTET STRING,  
  siteType SiteTopoSiteType,  
  siteLocation OCTET STRING,  
  siteLongitude OCTET STRING,  
  siteLatitude OCTET STRING,  
  siteTerritory OCTET STRING  
}

siteTopoSiteTable OBJECT-TYPE  
SYNTAX SEQUENCE OF SiteTopoSiteTableEntry  
MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION "Site topology site table. Lists the sites defined in the system and their parameters."
::= { cmConfigSiteTopology 2 }

siteTopoSiteTableEntry OBJECT-TYPE  
SYNTAX SiteTopoSiteTableEntry  
MAX-ACCESS not-accessible  
STATUS current  
DESCRIPTION "Site table entry."
INDEX { siteIndex }
::= { siteTopoSiteTable 1 }

siteIndex OBJECT-TYPE  
SYNTAX CmaDefaultTableIndexRange  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "Unique system-assigned ID for this entry."
::= { siteTopoSiteTableEntry 1 }

siteName OBJECT-TYPE  
SYNTAX OCTET STRING (SIZE(1..255))  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "Name of the site."
::= { siteTopoSiteTableEntry 2 }

siteDescription OBJECT-TYPE  
SYNTAX OCTET STRING (SIZE(1..255))

Polycom, Inc.
MAX-ACCESS  read-only
STATUS     current
DESCRIPTION “Description of the site.”
::= { siteTopoSiteTableEntry 3 }

siteOverrideItuDialingRules OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Flag indicating whether to override ITU dialing rules for the site.”
DEFVAL      { false }
::= { siteTopoSiteTableEntry 4 }

sitePbxAccessCode OBJECT-TYPE
SYNTAX      OCTET STRING (SIZE(0..10))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Access code required to enter the site's PBX system.”
DEFVAL      { "" }
::= { siteTopoSiteTableEntry 5 }

siteCountryCode OBJECT-TYPE
SYNTAX      OCTET STRING (SIZE(0..10))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Country code for the site.”
DEFVAL      { "" }
::= { siteTopoSiteTableEntry 6 }

siteAreaCode OBJECT-TYPE
SYNTAX      OCTET STRING (SIZE(0..10))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Area code for the site.”
DEFVAL      { "" }
::= { siteTopoSiteTableEntry 7 }

siteNumSubscriberDigits OBJECT-TYPE
SYNTAX      Integer32
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Number of digits in a phone number for the site.”
DEFVAL      { 0 }
::= { siteTopoSiteTableEntry 8 }

siteIsdnNumberAssignmentMethod OBJECT-TYPE
SYNTAX      SiteTopoIsdnNumberAssignmentMethodType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “ISDN number assignment method for the site.”
DEFVAL      { none }
::= { siteTopoSiteTableEntry 9 }

siteInternetRoutingType OBJECT-TYPE
SYNTAX      SiteTopoInternetRoutingType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Internet calling type for the site.”
DEFVAL      { notAllowed }
::= { siteTopoSiteTableEntry 10 }

siteSendDialStringtoSBCorALG OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Send unmodified Dial String to Session Border Controller(SBC) or Application Level Gateway(ALG)."
DEFVAL { false }
::= { siteTopoSiteTableEntry 11 }

siteCallSignallingInetAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address type for the site."
DEFVAL { ipv4 }
::= { siteTopoSiteTableEntry 12 }

siteCallSignallingInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address for the site."
DEFVAL { "" }
::= { siteTopoSiteTableEntry 13 }

siteSubnetCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of subnets defined for the site."
DEFVAL { 0 }
::= { siteTopoSiteTableEntry 19 }

siteIsdnGatewayPhoneNumber OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "ISDN gateway phone number for the site."
DEFVAL { "" }
::= { siteTopoSiteTableEntry 20 }

siteIsdnE164Start OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Start of the range of E.164 numbers available for automatic assignment to IP devices for the site."
DEFVAL { "" }
::= { siteTopoSiteTableEntry 21 }

siteIsdnE164End OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "End of the range of E.164 numbers available for automatic assignment to IP devices for the site."
DEFVAL { "" }
::= { siteTopoSiteTableEntry 22 }
siteIsdnC1iDigits OBJECT-TYPE
SYNTAX    Integer32(0..17)
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Number of digits in the Call Line Identifier, which is the dialed number for the site."
DEFVAL    { 0 }
::= { siteTopoSiteTableEntry 23 }

siteIsdnShortPhoneDigits OBJECT-TYPE
SYNTAX    Integer32
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Number of digits in the short form of the dialing number for the site. This number indicates what part of the dial string is sent to the gatekeeper for address resolution in gateway + extension dialing."
DEFVAL    { 0 }
::= { siteTopoSiteTableEntry 24 }

siteIsdnNumberRangeList OBJECT-TYPE
SYNTAX    OCTET STRING
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Comma-separated list of ISDN number ranges, specifying the ISDN numbers available for automatic assignment to IP devices for the site (each range has the format startNumber-endNumber)."
DEFVAL    { "" }
::= { siteTopoSiteTableEntry 25 }

siteType OBJECT-TYPE
SYNTAX    SiteTopoSiteType
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Type of site."
::= { siteTopoSiteTableEntry 26 }

siteLocation OBJECT-TYPE
SYNTAX    OCTET STRING
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Geo-location of site."
DEFVAL    { "" }
::= { siteTopoSiteTableEntry 27 }

siteLongitude OBJECT-TYPE
SYNTAX    OCTET STRING
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Geographical longitude of site."
DEFVAL    { "" }
::= { siteTopoSiteTableEntry 28 }

siteLatitude OBJECT-TYPE
SYNTAX    OCTET STRING
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Geographical latitude of site."
DEFVAL  { "" } ::= { siteTopoSiteTableEntry 29 }

siteTerritory OBJECT-TYPE
SYNTAX  OCTET STRING
MAX-ACCESS read-only
STATUS  current
DESCRIPTION "Territory that site belongs to."
DEFVAL  { "" } ::= { siteTopoSiteTableEntry 30 }

-- Links

siteTopoSiteLinkCount  OBJECT-TYPE
SYNTAX  Integer32
MAX-ACCESS read-only
STATUS  current
DESCRIPTION "Number of site links configured in CMA system."
 ::= { cmaConfigSiteTopology 3 }

SiteTopoSiteLinkTableEntry ::= SEQUENCE
{
  siteLinkIndex  CmaDefaultTableIndexRange,
  siteLinkName  OCTET STRING,
  siteLinkDescription  OCTET STRING,
  siteLinkSiteA  OCTET STRING,
  siteLinkSiteB  OCTET STRING,
  siteLinkTotalBandwidthRestriction  Counter64,
  siteLinkTotalBandwidthRestrictionEnabled  TruthValue,
  siteLinkMaxBitRateRestriction  Counter64,
  siteLinkMaxBitRateRestrictionEnabled  TruthValue
}

siteTopoSiteLinkTable OBJECT-TYPE
SYNTAX  SEQUENCE OF SiteTopoSiteLinkTableEntry
MAX-ACCESS not-accessible
STATUS  current
DESCRIPTION "Site topology site link table. Lists the site links defined in the system and their parameters."
 ::= { cmaConfigSiteTopology 4 }

siteTopoSiteLinkTableEntry OBJECT-TYPE
SYNTAX  SiteTopoSiteLinkTableEntry
MAX-ACCESS not-accessible
STATUS  current
DESCRIPTION "Site link table entry."
INDEX  { siteLinkIndex }
 ::= { siteTopoSiteLinkTableEntry 1 }

siteLinkIndex OBJECT-TYPE
SYNTAX  CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS  current
DESCRIPTION "Unique system-assigned ID for this entry."
 ::= { siteTopoSiteLinkTableEntry 1 }

siteLinkName OBJECT-TYPE
SYNTAX  OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS  current

Polycom, Inc.
DESCRIPTION "Name of the site link."
::= { siteTopoSiteLinkTableEntry 2 }

siteLinkDescription OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Description of the site link."
::= { siteTopoSiteLinkTableEntry 3 }

siteLinkSiteA OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the site of origin for the site link."
::= { siteTopoSiteLinkTableEntry 4 }

siteLinkSiteB OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the destination site for the site link."
::= { siteTopoSiteLinkTableEntry 5 }

siteLinkTotalBandwidthRestriction OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total bandwidth restriction for the site link."
::= { siteTopoSiteLinkTableEntry 6 }

siteLinkTotalBandwidthRestrictionEnabled OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether bandwidth is restricted for the site link."
::= { siteTopoSiteLinkTableEntry 7 }

siteLinkMaxBitRateRestriction OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Maximum call bit rate for the site link."
::= { siteTopoSiteLinkTableEntry 8 }

siteLinkMaxBitRateRestrictionEnabled OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether maximum call rate is restricted for the site link."
::= { siteTopoSiteLinkTableEntry 9 }

-- Subnets

siteTopoSubnetCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of subnets configured in CMA system." 
 ::= { cmaConfigSiteTopology 5 }

SiteTopoSubnetTableEntry ::= SEQUENCE
{
    subnetIndex CmaDefaultTableIndexRange,
    subnetName OCTET STRING,
    subnetSiteName OCTET STRING,
    subnetIpAddress InetAddress,
    subnetMaskSize Integer32,
    subnetTotalBandwidthRestriction Counter64,
    subnetTotalBandwidthRestrictionEnabled TruthValue,
    subnetMaxBitRateRestriction Counter64,
    subnetMaxBitRateRestrictionEnabled TruthValue
}

siteTopoSubnetTable OBJECT-TYPE
SYNTAX    SEQUENCE OF SiteTopoSubnetTableEntry
MAX-ACCESS not-accessible
STATUS    current
DESCRIPTION "Site topology subnet table. Lists the subnets defined in the system and their parameters."
 ::= { cmaConfigSiteTopology 6 }

siteTopoSubnetTableEntry OBJECT-TYPE
SYNTAX    SiteTopoSubnetTableEntry
MAX-ACCESS not-accessible
STATUS    current
DESCRIPTION "Subnet table entry."
INDEX    { subnetIndex }
 ::= { siteTopoSubnetTable 1 }

subnetIndex OBJECT-TYPE
SYNTAX    CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Unique system-assigned ID for this entry."
 ::= { siteTopoSubnetTableEntry 1 }

subnetName OBJECT-TYPE
SYNTAX    OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Name of the subnet."
 ::= { siteTopoSubnetTableEntry 2 }

subnetSiteName OBJECT-TYPE
SYNTAX    OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Name of the subnet's site."
 ::= { siteTopoSubnetTableEntry 3 }

subnetIpAddress OBJECT-TYPE
SYNTAX    InetAddress
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "IP address for the subnet."
 ::= { siteTopoSubnetTableEntry 4 }
subnetMaskSize OBJECT-TYPE
  SYNTAX Integer32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION "Bit size of the mask for the subnet."
  ::= { siteTopoSubnetTableEntry 5 }

subnetTotalBandwidthRestriction OBJECT-TYPE
  SYNTAX Counter64
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION "Bandwidth restriction for the subnet."
  ::= { siteTopoSubnetTableEntry 6 }

subnetTotalBandwidthRestrictionEnabled OBJECT-TYPE
  SYNTAX TruthValue
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION "Flag indicating whether bandwidth is restricted for the subnet."
  ::= { siteTopoSubnetTableEntry 7 }

subnetMaxBitRateRestriction OBJECT-TYPE
  SYNTAX Counter64
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION "Maximum call bit rate for the subnet."
  ::= { siteTopoSubnetTableEntry 8 }

subnetMaxBitRateRestrictionEnabled OBJECT-TYPE
  SYNTAX TruthValue
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION "Flag indicating whether maximum call rate is restricted for the subnet."
  ::= { siteTopoSubnetTableEntry 9 }

-- Clouds

siteTopoCloudCount OBJECT-TYPE
  SYNTAX Integer32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION "Number of network clouds configured in CMA system."
  ::= { cmaConfigSiteTopology 7 }

SiteTopoCloudTableEntry ::= SEQUENCE
  {
    cloudIndex CmaDefaultTableIndexRange,
    cloudName OCTET STRING,
    cloudDescription OCTET STRING
  }

siteTopoCloudTable OBJECT-TYPE
  SYNTAX SEQUENCE OF SiteTopoCloudTableEntry
  MAX-ACCESS not-accessible
  STATUS current
  DESCRIPTION "Site topology network cloud table. Lists the network clouds defined in the system and their parameters."
  ::= { cmaConfigSiteTopology 8 }
siteTopoCloudTableEntry OBJECT-TYPE
SYNTAX     SiteTopoCloudTableEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION "Cloud table entry."
INDEX      { cloudIndex }
 ::= { siteTopoCloudTableEntry 1 }

cloudIndex OBJECT-TYPE
SYNTAX     CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Unique system-assigned ID for this entry."
 ::= { siteTopoCloudTableEntry 1 }

cloudName OBJECT-TYPE
SYNTAX     OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Name of the network cloud."
 ::= { siteTopoCloudTableEntry 2 }

cloudDescription OBJECT-TYPE
SYNTAX     OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Description for the network cloud."
 ::= { siteTopoCloudTableEntry 3 }

-- Territories

siteTopoTerritoryCount OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Number of territories configured in CMA system."
 ::= { cmaConfigSiteTopology 9 }

SiteTopoTerritoryTableEntry ::= SEQUENCE
{
   territoryIndex                     CmaDefaultTableIndexRange,
   territoryName                      OCTET STRING,
   territoryDescription               OCTET STRING,
   territoryPrimaryNode               OCTET STRING,
   territoryBackupNode                OCTET STRING
}

siteTopoTerritoryTable OBJECT-TYPE
SYNTAX     SEQUENCE OF SiteTopoTerritoryTableEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION "Site topology territory table. Lists the territories defined in the system and their parameters."
 ::= { cmaConfigSiteTopology 10 }

siteTopoTerritoryTableEntry OBJECT-TYPE
SYNTAX     SiteTopoTerritoryTableEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION "Territory table entry."
INDEX { territoryIndex }
::= { siteTopoTerritoryTable 1 }

territoryIndex OBJECT-TYPE
SYNTAX CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Unique system-assigned ID for this entry."
::= { siteTopoTerritoryTableEntry 1 }

territoryName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the territory."
::= { siteTopoTerritoryTableEntry 2 }

territoryDescription OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Description for the territory."
::= { siteTopoTerritoryTableEntry 3 }

territoryPrimaryNode OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Primary node for the territory."
::= { siteTopoTerritoryTableEntry 4 }

territoryBackupNode OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Backup node for the territory."
::= { siteTopoTerritoryTableEntry 5 }

-- Site-to-Site Exclusions

siteTopoSiteToSiteExclusionCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of site-to-site exclusions configured in CMA system."
::= { cmConfigSiteTopology 11 }

SiteTopoSiteToSiteExclusionTableEntry ::= SEQUENCE
{
    siteToSiteExclusionIndex CmaDefaultTableIndexRange,
    siteToSiteExclusionSiteA OCTET STRING,
    siteToSiteExclusionSiteB OCTET STRING
}

siteTopoSiteToSiteExclusionTable OBJECT-TYPE
SYNTAX SEQUENCE OF SiteTopoSiteToSiteExclusionTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "Site topology site-to-site exclusion table. Lists the site-to-site exclusions"
defined in the system and their parameters.
 ::= { cmaConfigSiteTopology 12 }

siteTopoSiteToSiteExclusionTableEntry OBJECT-TYPE
SYNTAX    SiteTopoSiteToSiteExclusionTableEntry
MAX-ACCESS not-accessible
STATUS    current
DESCRIPTION “Site-to-site table entry.”
INDEX     { siteToSiteExclusionIndex }
 ::= { siteTopoSiteToSiteExclusionTable 1 }

siteToSiteExclusionIndex OBJECT-TYPE
SYNTAX    CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS    current
DESCRIPTION “Unique system-assigned ID for this entry.”
 ::= { siteTopoSiteToSiteExclusionTableEntry 1 }

siteToSiteExclusionSiteA OBJECT-TYPE
SYNTAX    OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS    current
DESCRIPTION “Site A for the site-to-site exclusion.”
 ::= { siteTopoSiteToSiteExclusionTableEntry 2 }

siteToSiteExclusionSiteB OBJECT-TYPE
SYNTAX    OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS    current
DESCRIPTION “Site B for the site-to-site exclusion.”
 ::= { siteTopoSiteToSiteExclusionTableEntry 3 }

-- Site Provisioning
sitetopologySiteProvisioningCount  OBJECT-TYPE
SYNTAX    Integer32
MAX-ACCESS read-only
STATUS    current
DESCRIPTION “Number of site provisioning profiles configured in CMA system.”
 ::= { cmaConfigSiteProvisioning 1 }

SiteTopologySiteProvisioningDetailsTableEntry ::= SEQUENCE
{  
siteProvisioningSiteName OCTET STRING,
siteCountry OCTET STRING,
siteDateFormat SiteProvisioningDateFormatType,
siteAutoAdjustDst TruthValue,
siteTimeFormat SiteProvisioningTimeFormatType,
siteTimeServerUpdateType SiteTimeServerUpdateType,
sitePrimaryTimeServerInetAddressType InetAddressType,
sitePrimaryTimeServerInetAddress InetAddress,
siteSecondaryTimeServerInetAddressType InetAddressType,
siteSecondaryTimeServerInetAddress InetAddress,
siteTimeZone CmaTimeZone,
siteFirewallUseFixedPorts TruthValue,
siteFirewallTcpStartPort InetPortNumber,
siteFirewallUdpStartPort InetPortNumber,
siteFirewallH460Traversal TruthValue,
siteFirewallNatConfiguration SiteNatConfigurationType,
}
siteFirewallNatWanAddressType InetAddressType,
siteFirewallNatWanAddress InetAddress,
siteFirewallNatH323Compatible TruthValue,
siteFirewallShowEpInGab TruthValue,
siteFirewallEnableSipKeepAlives TruthValue,
siteH323EnableIpCalls TruthValue,
siteH323GatekeeperIPAddressType InetAddressType,
siteH323GatekeeperIPAddress InetAddress,
siteH3232UseGkForMultipointCalls SiteUseGkForMultipointCallsType,
siteProvisioningPollingInterval Integer32,
siteSoftupdatePollingInterval Integer32,
siteQosVideoTosValue Integer32,
siteQosAudioTosValue Integer32,
siteQosFecTosValue Integer32,
siteQosType SiteQosTypeOfServiceType,
siteQosMaxMtuSize SiteQosMtuSizeType,
siteQosEnablePvec TruthValue,
siteQosEnableRsvp TruthValue,
siteQosDynamicBandwidth TruthValue,
siteQosMaxTransmitBandwidth SiteQosBandwidthType,
siteQosMaxReceiveBandwidth SiteQosBandwidthType,
siteSecurityUsePwdForRemoteAccess TruthValue,
siteSecurityEnableSecureMode TruthValue,
siteSecurityEnableEncryption SiteSecurityEnableEncryptionType,
siteSecurityEnableWebAccess TruthValue,
siteSecurityEnableTelnetAccess TruthValue,
siteSecurityEnableSmpAccess TruthValue,
siteSecurityWebAccessPort InetPortNumber,
siteSecurityAllowWebVideoDisplay TruthValue,
siteSecurityNtlmVersion OCTET STRING,
cmadHeartbeatPollingInterval Integer32,
cmadInCallStatsPollingInterval Integer32,
siteCalendaringExchangeServerIPAddressType InetAddressType,
siteCalendaringExchangeServerIPAddress InetAddress,
siteSIPEnable TruthValue,
siteSIPDomain OCTET STRING,
siteSIPAutoDiscoverServer TruthValue,
siteSIPProxyServerInetAddressType InetAddressType,
siteSIPProxyServerInetAddress InetAddress,
siteSIPRegistrarServerInetAddressType InetAddressType,
siteSIPRegistrarServerInetAddress InetAddress,
siteSIPBackupProxyServerInetAddressType InetAddressType,
siteSIPBackupProxyServerInetAddress InetAddress,
siteSIPBackupRegistrarServerInetAddressType InetAddressType,
siteSIPBackupRegistrarServerInetAddress InetAddress,
siteSIPTransportLayerProtocol SiteSIPTransportProtocolType,
siteSIPServerType SiteSIPServerType,
siteSIPVerifyCertificate TruthValue,
siteSIPUseEnterpriseCredentials TruthValue,
siteSecurityProfile OCTET STRING,
siteSecurityIdleSessionTimeout Integer32,
siteSecurityFailedLoginThreshold Integer32,
siteSecurityFailedLoginWindow Integer32,
siteSecurityPortLockoutDuration Integer32,
siteSecurityMaxCertificateVerificationDepth Integer32,
siteSecurityVerifyCertificateForWebAccess TruthValue,
siteWhitelistIPEnable TruthValue,
siteEnableEnterpriseDir TruthValue,
siteEnterpriseDirAdminGroup OCTET STRING,
siteEnterpriseDirUserGroup OCTET STRING,
MIB Reference

```
siteDirectorySettingsUseThisServer                 TruthValue,
siteDirectorySettingsServerIPAddress             InetAddress,
siteDirectorySettingsVerifyCertificate          TruthValue,
sitePresenceSettingsUseThisServer               TruthValue,
sitePresenceSettingsServerIPAddress             InetAddress,
sitePresenceSettingsVerifyCertificate          TruthValue
}
sitetopologySiteProvisioningTable OBJECT-TYPE
  SYNTAX        SEQUENCE OF SiteTopologySiteProvisioningDetailsTableEntry
  MAX-ACCESS    not-accessible
  STATUS        current
  DESCRIPTION   "Site topology site provisioning details table. Contains the provisioning details for each site."
  ::= { cmaConfigSiteProvisioning 2 }
siteTopologySiteProvisioningDetailsTableEntry OBJECT-TYPE
  SYNTAX        SiteTopologySiteProvisioningDetailsTableEntry
  MAX-ACCESS    not-accessible
  STATUS        current
  DESCRIPTION   "Site provisioning details entry."
  INDEX         { siteIndex }
  ::= { sitetopologySiteProvisioningTable 1 }
siteProvisioningSiteName OBJECT-TYPE
  SYNTAX      OCTET STRING (SIZE(1..255))
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION "Name of the site."
  ::= { siteTopologySiteProvisioningDetailsTableEntry 1 }
siteCountry    OBJECT-TYPE
  SYNTAX      OCTET STRING
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION "Country of the site."
  ::= { siteTopologySiteProvisioningDetailsTableEntry 2 }
siteDateFormat   OBJECT-TYPE
  SYNTAX      SiteProvisioningDateFormatType
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION "Date format for the site."
  ::= { siteTopologySiteProvisioningDetailsTableEntry 3 }
siteAutoAdjustDst   OBJECT-TYPE
  SYNTAX      TruthValue
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION "Flag indicating whether to adjust the site's endpoint system clocks for daylight saving time."
  ::= { siteTopologySiteProvisioningDetailsTableEntry 4 }
siteTimeFormat   OBJECT-TYPE
  SYNTAX      SiteProvisioningTimeFormatType
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION "Time format for the site."
  ::= { siteTopologySiteProvisioningDetailsTableEntry 5 }
```
siteTimeServerUpdateType  OBJECT-TYPE
SYNTAX      SiteTimeServerUpdateType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Time format for the site.”
::= { siteTopologySiteProvisioningDetailsTableEntry 6 }

sitePrimaryTimeServerInetAddressType  OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “IP address type of the primary time server for the site.”
::= { siteTopologySiteProvisioningDetailsTableEntry 7 }

sitePrimaryTimeServerInetAddress   OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “IP address of the primary time server for the site.”
::= { siteTopologySiteProvisioningDetailsTableEntry 8 }

siteSecondaryTimeServerInetAddressType  OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “IP address type of the secondary time server for the site.”
::= { siteTopologySiteProvisioningDetailsTableEntry 9 }

siteSecondaryTimeServerInetAddress   OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “IP address of the secondary time server for the site.”
::= { siteTopologySiteProvisioningDetailsTableEntry 10 }

siteTimeZone   OBJECT-TYPE
SYNTAX      CmaTimeZone
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Time zone for the site.”
::= { siteTopologySiteProvisioningDetailsTableEntry 11 }

siteFirewallUseFixedPorts   OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Flag indicating whether the TCP and UDP ports to use are defined for the site.”
::= { siteTopologySiteProvisioningDetailsTableEntry 12 }

siteFirewallTcpStartPort   OBJECT-TYPE
SYNTAX      InetPortNumber
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION “Starting TCP port number used by the site's endpoint systems.”
::= { siteTopologySiteProvisioningDetailsTableEntry 13 }

siteFirewallUdpStartPort   OBJECT-TYPE
SYNTAX      InetPortNumber
MAX-ACCESS  read-only
MIB Reference

STATUS current
DESCRIPTION "Starting UDP port number used by the site's endpoint systems."
::= { siteTopologySiteProvisioningDetailsTableEntry 14 }

siteFirewallH460Traversal OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the site's endpoint systems are allowed to use H.460-based firewall traversal."
::= { siteTopologySiteProvisioningDetailsTableEntry 15 }

siteFirewallNatConfiguration OBJECT-TYPE
SYNTAX SiteNatConfigurationType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the site's endpoint systems should determine the NAT public (WAN) address automatically."
::= { siteTopologySiteProvisioningDetailsTableEntry 16 }

siteFirewallNatWanAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Address type of the NAT public (WAN) IP address for the site. Only valid if the siteFirewallNatConfiguration attribute is set to manual."
::= { siteTopologySiteProvisioningDetailsTableEntry 17 }

siteFirewallNatWanAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "NAT public (WAN) IP address for the site. Only valid if the siteFirewallNatConfiguration attribute is set to manual."
::= { siteTopologySiteProvisioningDetailsTableEntry 18 }

siteFirewallNatH323Compatible OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the site's endpoint systems are behind a NAT capable of translating H.323 traffic."
::= { siteTopologySiteProvisioningDetailsTableEntry 19 }

siteFirewallShowEpInGab OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether endpoint system information is to be included in the global directory for the site."
::= { siteTopologySiteProvisioningDetailsTableEntry 20 }

siteFirewallEnableSipKeepAlives OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether SIP Keep Alives will be enabled for the site"
::= { siteTopologySiteProvisioningDetailsTableEntry 21 }
siteH323EnableIpCalls OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether IP H.323 calls are enabled for the site."
 ::= { siteTopologySiteProvisioningDetailsTableEntry 22 }

siteH323GatekeeperIPAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address type of the gatekeeper for the site.
Only valid if the siteH323EnableIpCalls attribute is true."
 ::= { siteTopologySiteProvisioningDetailsTableEntry 24 }

siteH323GatekeeperIPAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the gatekeeper for the site.
Only valid if the siteH323EnableIpCalls attribute is true."
 ::= { siteTopologySiteProvisioningDetailsTableEntry 25 }

siteH323UseGkForMultipointCalls OBJECT-TYPE
SYNTAX SiteUseGkForMultipointCallsType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the site's multipoint calls use the endpoint system's
internal multipoint capability or the Polycom MCUs' conference on demand feature."
 ::= { siteTopologySiteProvisioningDetailsTableEntry 26 }

siteProvisioningPollingInterval OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Frequency in minutes at which the site's endpoint systems poll the CMA
for new provisioning information."
 ::= { siteTopologySiteProvisioningDetailsTableEntry 27 }

siteSoftupdatePollingInterval OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Frequency in minutes at which the site's endpoint systems poll the CMA
for a new softupdate package."
 ::= { siteTopologySiteProvisioningDetailsTableEntry 28 }

siteQosVideoTosValue OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP precedence or Diffserv value for the site's video packets."
 ::= { siteTopologySiteProvisioningDetailsTableEntry 29 }

siteQosAudioTosValue OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP precedence or Diffserv value for the site's audio packets."
::= { siteTopologySiteProvisioningDetailsTableEntry 30 }

siteQosFeccTosValue OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP precedence or Diffserv value for the site's Far End Camera Control packets."
::= { siteTopologySiteProvisioningDetailsTableEntry 31 }

siteQosTosType OBJECT-TYPE
SYNTAX SiteQosTypeOfServiceType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Type of service (IP precedence or Diffserv) for the site's audio, video, and FECC TOS values."
::= { siteTopologySiteProvisioningDetailsTableEntry 32 }

siteQosMaxMtuSize OBJECT-TYPE
SYNTAX SiteQosMtuSizeType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Maximum transmission unit (MTU) size in bytes used in IP calls for the site."
::= { siteTopologySiteProvisioningDetailsTableEntry 33 }

siteQosEnablePvec OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the site's endpoint systems can use Polycom Video Error Concealment (PVEC) if packet loss occurs."
::= { siteTopologySiteProvisioningDetailsTableEntry 34 }

siteQosEnableRsvp OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the site's endpoint systems can use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path."
::= { siteTopologySiteProvisioningDetailsTableEntry 35 }

siteQosDynamicBandwidth OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the site's endpoint systems automatically find the optimum line speed for a call."
::= { siteTopologySiteProvisioningDetailsTableEntry 36 }

siteQosMaxTransmitBandwidth OBJECT-TYPE
SYNTAX SiteQosBandwidthType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Maximum transmission line speed for the site in Kbps."
::= { siteTopologySiteProvisioningDetailsTableEntry 37 }

siteQosMaxReceiveBandwidth OBJECT-TYPE
SYNTAX SiteQosBandwidthType

Polycom, Inc.
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Maximum reception line speed for the site in Kbps."
::= { siteTopologySiteProvisioningDetailsTableEntry 38 }

siteSecurityUsePwdForRemoteAccess OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the local endpoint system password and remote access password are the same for the site."
::= { siteTopologySiteProvisioningDetailsTableEntry 39 }

siteSecurityEnableSecureMode OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether to operate in secure mode with the site's devices."
::= { siteTopologySiteProvisioningDetailsTableEntry 40 }

siteSecurityEnableEncryption OBJECT-TYPE
SYNTAX SiteSecurityEnableEncryptionType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Encryption usage setting for the site."
::= { siteTopologySiteProvisioningDetailsTableEntry 41 }

siteSecurityEnableWebAccess OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether to allow web access to the site's endpoint systems."
::= { siteTopologySiteProvisioningDetailsTableEntry 42 }

siteSecurityEnableTelnetAccess OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether to allow telnet access to the site's endpoint systems."
::= { siteTopologySiteProvisioningDetailsTableEntry 43 }

siteSecurityEnableSnmpAccess OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether to allow SNMP access to the site's endpoint systems."
::= { siteTopologySiteProvisioningDetailsTableEntry 44 }

siteSecurityWebAccessPort OBJECT-TYPE
SYNTAX InetPortNumber
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Port number to use when accessing an endpoint system's web interface."
::= { siteTopologySiteProvisioningDetailsTableEntry 45 }
MIB Reference

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>siteSecurityAllowWebVideoDisplay</td>
<td>Flag indicating whether to allow viewing of the endpoint video using the endpoint system's web interface.</td>
</tr>
<tr>
<td>siteSecurityNtlmVersion</td>
<td>NTLM version setting for the site.</td>
</tr>
<tr>
<td>siteCmadHeartbeatPollingInterval</td>
<td>Frequency in minutes at which the site's endpoint systems poll the CMA system for a heartbeat.</td>
</tr>
<tr>
<td>siteCmadInCallStatsPollingInterval</td>
<td>Frequency in minutes at which the site's endpoint systems poll the CMA system for in-call statistics.</td>
</tr>
<tr>
<td>siteCalendaringExchangeServerIPAddressType</td>
<td>IP address type of the Exchange server for the site.</td>
</tr>
<tr>
<td>siteCalendaringExchangeServerIPAddress</td>
<td>IP address of the Exchange server for the site.</td>
</tr>
<tr>
<td>siteSIPEnable</td>
<td>Flag indicating whether SIP is enabled or.</td>
</tr>
<tr>
<td>siteSIPDomain</td>
<td>Name of the SIP Domain.</td>
</tr>
</tbody>
</table>

---

Polycom, Inc. 579
siteSIPAutoDiscoverServer  OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "Flag indicating whether autodiscovering SIP Server is Enabled."
 ::= { siteTopologySiteProvisioningDetailsTableEntry 54 }

siteSIPProxyServerInetAddressType  OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "IP address type for the SIP Proxy Server."
DEFVAL      { ipv4 }
 ::= { siteTopologySiteProvisioningDetailsTableEntry 55 }

siteSIPProxyServerInetAddress  OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "IP address for the SIP Proxy Server."
DEFVAL      { "" }
 ::= { siteTopologySiteProvisioningDetailsTableEntry 56 }

siteSIPRegistrarServerInetAddressType  OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "IP address type for the SIP Registrar Server."
DEFVAL      { ipv4 }
 ::= { siteTopologySiteProvisioningDetailsTableEntry 57 }

siteSIPRegistrarServerInetAddress  OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "IP address for the SIP Registrar Server."
DEFVAL      { "" }
 ::= { siteTopologySiteProvisioningDetailsTableEntry 58 }

siteSIPBackupProxyServerInetAddressType  OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "IP address type for the SIP Backup Proxy Server."
DEFVAL      { ipv4 }
 ::= { siteTopologySiteProvisioningDetailsTableEntry 59 }

siteSIPBackupProxyServerInetAddress  OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "IP address for the SIP Backup Proxy Server."
DEFVAL      { "" }
 ::= { siteTopologySiteProvisioningDetailsTableEntry 60 }

siteSIPBackupRegistrarServerInetAddressType  OBJECT-TYPE
SYNTAX      InetAddressType
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "IP address type for the SIP Backup Registrar Server."
DEFVAL      { ipv4 }
 ::= { siteTopologySiteProvisioningDetailsTableEntry 61 }
STATUS current
DESCRIPTION "IP address type for the SIPBackupRegistrarServer."
DEFVAL { ipv4 }
::= { siteTopologySiteProvisioningDetailsTableEntry 61 }

siteSIPBackupRegistrarServerInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address for the SIPBackupRegistrarServer."
DEFVAL { "" }
::= { siteTopologySiteProvisioningDetailsTableEntry 62 }

siteSIPTransportLayerProtocol OBJECT-TYPE
SYNTAX SiteSIPTransportProtocolType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Transport Layer Protocol for the SIP."
::= { siteTopologySiteProvisioningDetailsTableEntry 63 }

siteSIPServerType OBJECT-TYPE
SYNTAX SiteSIPServerType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "SIP Server type for SIP Protocol ."
::= { siteTopologySiteProvisioningDetailsTableEntry 64 }

siteSIPVerifyCertificate OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating if the certificates are verified."
::= { siteTopologySiteProvisioningDetailsTableEntry 65 }

siteSIPUseEnterpriseCredentials OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether Enterprise Directory Credentials are used for login."
::= { siteTopologySiteProvisioningDetailsTableEntry 66 }

siteSecurityProfile OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Security Profile Selected for this site ."
::= { siteTopologySiteProvisioningDetailsTableEntry 67 }

siteSecurityIdleSessionTimeout OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Idle session Timeout in Minutes."
::= { siteTopologySiteProvisioningDetailsTableEntry 68 }

siteSecurityFailedLoginThreshold OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Lock Port after Failed Logins, zero is off"
::= { siteTopologySiteProvisioningDetailsTableEntry 69 }

siteSecurityFailedLoginWindow OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Failed Login Window in hours."
::= { siteTopologySiteProvisioningDetailsTableEntry 71 }

siteSecurityPortLockoutDuration OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Port Lockout duration in minutes."
::= { siteTopologySiteProvisioningDetailsTableEntry 72 }

siteSecurityMaxCertificateVerificationDepth OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Maximum Peer Certificate Verification Depth."
::= { siteTopologySiteProvisioningDetailsTableEntry 73 }

siteSecurityVerifyCertForWebAccess OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether certificates are to be verified for all Web Accesses."
::= { siteTopologySiteProvisioningDetailsTableEntry 74 }

siteWhiteListIPEnable OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether WhiteList for IP's is enabled."
::= { siteTopologySiteProvisioningDetailsTableEntry 75 }

siteEnterpriseDirAdminGroup OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the Enterprise Directory Admin Group."
::= { siteTopologySiteProvisioningDetailsTableEntry 76 }

siteEnterpriseDirUserGroup OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the Enterprise Directory User Group."
::= { siteTopologySiteProvisioningDetailsTableEntry 77 }

siteDirectorySettingsUseThisServer OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether use this server for Directory server."
::= { siteTopologySiteProvisioningDetailsTableEntry 78 }

siteDirectorySettingsServerIPAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the Directory server for the site."
::= { siteTopologySiteProvisioningDetailsTableEntry 79 }

siteDirectorySettingsVerifyCertificate OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether Verify Certificate is enabled for this site."
::= { siteTopologySiteProvisioningDetailsTableEntry 80 }

sitePresenceSettingsUseThisServer OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether use this server for Presence server."
::= { siteTopologySiteProvisioningDetailsTableEntry 81 }

sitePresenceSettingsServerIPAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the Presence server for the site."
::= { siteTopologySiteProvisioningDetailsTableEntry 82 }

sitePresenceSettingsVerifyCertificate OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether Verify Certificate is enabled for this site."
::= { siteTopologySiteProvisioningDetailsTableEntry 83 }

-- END Site topology

-- SAM Site Provisioning BEGIN
sitetopologySAMSiteProvisioningCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of SAM site provisioning profiles configured in CMA system."
::= { cmaConfigSiteProvisioning 3 }

SAMSiteTopologySiteProvisioningDetailsTableEntry ::= SEQUENCE
{
  samsiteProvisioningSiteName OCTET STRING,
  samsiteTimeServerUpdateType SiteTimeServerUpdateType,
  samsitePrimaryTimeServerInetAddressType InetAddressType,
  samsitePrimaryTimeServerInetAddress InetAddress,
  samsiteSecondaryTimeServerInetAddressType InetAddressType,
  samsiteSecondaryTimeServerInetAddress InetAddress,
  samsiteProvisioningPollingInterval Integer32,
}
samsiteCmadHeartbeatPollingInterval  Integer32,
samserverStatusPollingInterval  Integer32,

samsiteH323EnableIpCalls  TruthValue,
samsiteH323GatekeeperIPAddressType  InetAddressType,
samsiteH323GatekeeperIPAddress  InetAddress,

samsiteSIPEnable  TruthValue,
samsiteSIPProxyServerInetAddressType  InetAddressType,
samsiteSIPProxyServerInetAddress  InetAddress,
samsiteSIPRegistrarServerInetAddressType  InetAddressType,
samsiteSIPRegistrarServerInetAddress  InetAddress,
samsiteSIPTransportLayerProtocol  SiteSIPTransportProtocolType,
samsiteSIPVerifyCertificate  TruthValue,

samsiteDirectorySettingsUseThisServer  TruthValue,
samsiteDirectorySettingsServerIPAddress  InetAddress,
samsiteDirectorySettingsVerifyCertificate  TruthValue,
samsitePresenceSettingsUseThisServer  TruthValue,
samsitePresenceSettingsServerIPAddress  InetAddress,
samsitePresenceSettingsVerifyCertificate  TruthValue

sitetopologySAMSiteProvisioningTable OBJECT-TYPE
SYNTAX  SEQUENCE OF SAMSiteTopologySiteProvisioningDetailsTableEntry
MAX-ACCESS  not-accessible
STATUS  current
DESCRIPTION  “Site topology SAM site provisioning details table.
Contains the provisioning details for each site.”
 ::= { cmaConfigSiteProvisioning 4 }

samSiteTopologySiteProvisioningDetailsTableEntry OBJECT-TYPE
SYNTAX  SAMSiteTopologySiteProvisioningDetailsTableEntry
MAX-ACCESS  not-accessible
STATUS  current
DESCRIPTION  “SAM Site provisioning details entry.”
INDEX  { siteIndex }
 ::= { sitetopologySAMSiteProvisioningTable 1 }

samsiteProvisioningSiteName OBJECT-TYPE
SYNTAX  OCTET STRING (SIZE(1..255))
MAX-ACCESS  read-only
STATUS  current
DESCRIPTION  “Name of the site.”
 ::= { samSiteTopologySiteProvisioningDetailsTableEntry 1 }

samsiteTimeServerUpdateType  OBJECT-TYPE
SYNTAX  SiteTimeServerUpdateType
MAX-ACCESS  read-only
STATUS  current
DESCRIPTION  “Time format for the sam site.”
 ::= { samSiteTopologySiteProvisioningDetailsTableEntry 2 }

samsitePrimaryTimeServerInetAddressType  OBJECT-TYPE
SYNTAX  InetAddressType
MAX-ACCESS  read-only
STATUS  current
DESCRIPTION  “IP address type of the primary time server for the sam site.”
 ::= { samSiteTopologySiteProvisioningDetailsTableEntry 3 }
samsitePrimaryTimeServerInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the primary time server for the sam site."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 4 }

samsiteSecondaryTimeServerInetAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address type of the secondary time server for the sam site."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 5 }

samsiteSecondaryTimeServerInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the secondary time server for the sam site."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 6 }

samsiteProvisioningPollingInterval OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Frequency at which the site's endpoint systems poll the CMA for new provisioning information."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 7 }

samsiteCmadHeartbeatPollingInterval OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Frequency at which the site's endpoint systems poll the CMA system for a heartbeat."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 8 }

samserverStatusPollingInterval OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Frequency at which the site's endpoint systems poll the CMA system for a server status"
::= { samSiteTopologySiteProvisioningDetailsTableEntry 9 }

samsiteH323EnableIpCalls OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether IP H.323 calls are enabled for the site."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 10 }

samsiteH323GatekeeperIPAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address type of the gatekeeper for the site. Only valid if the siteH323EnableIpCalls attribute is true."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 11 }
samsiteH323GatekeeperIPAddress  OBJECT-TYPE
   SYNTAX      InetAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IP address of the gatekeeper for the site. Only valid if
                the siteH323EnableIpCalls attribute is true."
   ::= { samSiteTopologySiteProvisioningDetailsTableEntry 12 }

samsiteSIPEnable  OBJECT-TYPE
   SYNTAX      TruthValue
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Flag indicating whether SIP is Enabled or."
   ::= { samSiteTopologySiteProvisioningDetailsTableEntry 13 }

samsiteSIPProxyServerInetAddressType  OBJECT-TYPE
   SYNTAX      InetAddressType
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IP address type for the SIP Proxy Server."
   DEFVAL { ipv4 }
   ::= { samSiteTopologySiteProvisioningDetailsTableEntry 14 }

samsiteSIPProxyServerInetAddress  OBJECT-TYPE
   SYNTAX      InetAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IP address for the SIP Proxy Server."
   DEFVAL { "" }
   ::= { samSiteTopologySiteProvisioningDetailsTableEntry 15 }

samsiteSIPRegistrarServerInetAddressType  OBJECT-TYPE
   SYNTAX      InetAddressType
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IP address type for the SIP Registrar Server."
   DEFVAL { ipv4 }
   ::= { samSiteTopologySiteProvisioningDetailsTableEntry 16 }

samsiteSIPRegistrarServerInetAddress  OBJECT-TYPE
   SYNTAX      InetAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IP address for the SIP Registrar Server."
   DEFVAL { "" }
   ::= { samSiteTopologySiteProvisioningDetailsTableEntry 17 }

samsiteSIPTransportLayerProtocol  OBJECT-TYPE
   SYNTAX      SiteSIPTransportProtocolType
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Transport Layer Protocol for the SIP."
   ::= { samSiteTopologySiteProvisioningDetailsTableEntry 18 }

samsiteSIPVerifyCertificate  OBJECT-TYPE
   SYNTAX      TruthValue
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Flag indicating if the certificates are verified."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 19 }

samsiteDirectorySettingsUseThisServer OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether use this server for Directory server."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 20 }

samsiteDirectorySettingsServerIPAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the Directory server for the site."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 21 }

samsiteDirectorySettingsVerifyCertificate OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether Verify Certificate is enabled for this site."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 22 }

samsitePresenceSettingsUseThisServer OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether use this server for Presence server."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 23 }

samsitePresenceSettingsServerIPAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the Presence server for the site."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 24 }

samsitePresenceSettingsVerifyCertificate OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether Verify Certificate is enabled for this site."
::= { samSiteTopologySiteProvisioningDetailsTableEntry 25 }

-- SAM Site Provisioning END

-- START conference settings configuration
cmaConferenceSettingGroup OBJECT-GROUP
OBJECTS
{
cmaConferenceConfigTimeWarning,
cmaConferenceConfigIncludeScheduler,
cmaConferenceConfigAllowOverbookForDial-in,
cmaConferenceConfigPasscodeLength
}
STATUS current
DESCRIPTION "CMA conference settings conformance group."
::= { cmaConfigConformance 16 }
cmaConferenceConfigTimeWarning OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether a message is sent to video endpoint systems to let users know that the conference is ending soon."
 ::= { cmaConfigConferenceGeneral 1 }

cmaConferenceConfigIncludeScheduler OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the conference scheduler is automatically added to a new conference."
 ::= { cmaConfigConferenceGeneral 2 }

cmaConferenceConfigAllowOverbookForDial-in OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether over-booking Dial-in Participants is allowed for a particular conference."
 ::= { cmaConfigConferenceGeneral 3 }

cmaConferenceConfigPasscodeLength OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Conference and chairperson passcode length."
 ::= { cmaConfigConferenceGeneral 4 }

-- END conference settings configuration

-- START Room configuration

cmaConfigRoomGroup OBJECT-GROUP
OBJECTS
{ cmaConfigRoomCount, roomIndex, roomName, roomDescription, roomSite, roomEmailAddress }
STATUS current
DESCRIPTION "CMA room configuration conformance group."
 ::= { cmaConfigConformance 18 }

cmaConfigRoomCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of configured rooms."
 ::= { cmaConfigRooms 1 }

CmaConfigRoomTableEntry ::= SEQUENCE
{ roomIndex CmaDefaultTableIndexRange,
roomName OCTET STRING,
roomDescription OCTET STRING,
roomSite OCTET STRING,
roomEmailAddress OCTET STRING
}

cmaConfigRoomTable OBJECT-TYPE
SYNTAX       SEQUENCE OF CmaConfigRoomTableEntry
MAX-ACCESS   not-accessible
STATUS       current
DESCRIPTION   "CMA room table. Contains information about the rooms defined in the system."
::= { cmaConfigRooms 2 }

cmaConfigRoomTableEntry OBJECT-TYPE
SYNTAX       CmaConfigRoomTableEntry
MAX-ACCESS   not-accessible
STATUS       current
DESCRIPTION   "Room configuration table entry."
INDEX        { roomIndex }
::= { cmaConfigRoomTable 1 }

roomIndex OBJECT-TYPE
SYNTAX       CmaDefaultTableIndexRange
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION   "Unique system-assigned ID for this entry."
::= { cmaConfigRoomTableEntry 1 }

roomName OBJECT-TYPE
SYNTAX       OCTET STRING (SIZE(0..255))
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION   "Name of the room."
::= { cmaConfigRoomTableEntry 2 }

roomDescription OBJECT-TYPE
SYNTAX       OCTET STRING (SIZE(0..255))
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION   "Description of the room."
::= { cmaConfigRoomTableEntry 3 }

roomSite OBJECT-TYPE
SYNTAX       OCTET STRING (SIZE(0..255))
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION   "Name of the site in which the room is located."
::= { cmaConfigRoomTableEntry 4 }

roomEmailAddress OBJECT-TYPE
SYNTAX       OCTET STRING (SIZE(0..255))
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION   "Email address for the room."
::= { cmaConfigRoomTableEntry 5 }

-- END Room configuration

-- START SNMP configuration
cmaConfigSnmpGroup OBJECT-GROUP
   OBJECTS
   {
      snmpVersion,
      snmpTransport,
      snmpPort,
      snmpCommunity,
      snmpV3ContextName,
      snmpV3SecurityUser,
      snmpAuthenticationType,
      snmpEncryptionType,
      snmpV3LocalEngineId,
      recipientIndex,
      recipientIPAddressType,
      recipientIPAddress,
      recipientPort,
      recipientTransportType,
      recipientNotificationType,
      recipientSnmpVersion,
      recipientSecurityUser,
      recipientAuthenticationType,
      recipientEncryptionType
   }
   STATUS current
   DESCRIPTION "CMA SNMP configuration conformance group."
   ::= { cmaConfigConformance 22 }

snmpVersion OBJECT-TYPE
   SYNTAX  SnmpVersionType
   MAX-ACCESS read-only
   STATUS   current
   DESCRIPTION "SNMP version."
   ::= { cmaConfigSnmp 1 }

snmpTransport OBJECT-TYPE
   SYNTAX  SnmpTransportType
   MAX-ACCESS read-only
   STATUS   current
   DESCRIPTION "Type of transport used for SNMP."
   ::= { cmaConfigSnmp 2 }

snmpPort OBJECT-TYPE
   SYNTAX  InetPortNumber
   MAX-ACCESS read-only
   STATUS   current
   DESCRIPTION "Port used for SNMP."
   ::= { cmaConfigSnmp 3 }

snmpCommunity OBJECT-TYPE
   SYNTAX  OCTET STRING (SIZE(0..255))
   MAX-ACCESS read-only
   STATUS   current
   DESCRIPTION "SNMP v2 community name."
   ::= { cmaConfigSnmp 4 }

snmpV3ContextName OBJECT-TYPE
   SYNTAX  OCTET STRING (SIZE(0..255))
   MAX-ACCESS read-only
   STATUS   current
   DESCRIPTION "SNMP v3 context name."
::= { cmaConfigSnmp 5 }

snmpV3SecurityUser OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "SNMP v3 security user name."
 ::= { cmaConfigSnmp 6 }

snmpAuthenticationType OBJECT-TYPE
SYNTAX SnmpAuthenticationType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "SNMP v3 authentication type."
 ::= { cmaConfigSnmp 7 }

snmpEncryptionType OBJECT-TYPE
SYNTAX SnmpEncryptionType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "SNMP v3 encryption type."
 ::= { cmaConfigSnmp 8 }

snmpV3LocalEngineId OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "SNMP v3 local engine ID."
 ::= { cmaConfigSnmp 9 }

SnmpNoticationRecipientTableEntry ::= SEQUENCE
{
  recipientIndex CmaDefaultTableIndexRange,
  recipientIPAddressType InetAddressType,
  recipientIPAddress InetAddress,
  recipientPort InetPortNumber,
  recipientTransportType SnmpTransportType,
  recipientNotificationType SnmpNotificationType,
  recipientSnmpVersion SnmpVersionType,
  recipientSecurityUser OCTET STRING,
  recipientAuthenticationType SnmpAuthenticationType,
  recipientEncryptionType SnmpEncryptionType
}

snmpNoticationRecipientTable OBJECT-TYPE
SYNTAX SEQUENCE OF SnmpNoticationRecipientTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "SNMP notification recipients table. Each entry contains the parameters for
an agent that receives notifications from the CMA server."
 ::= { cmaConfigSnmp 10 }

snmpNoticationRecipientTableEntry OBJECT-TYPE
SYNTAX SnmpNoticationRecipientTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "SNMP notification recipient table entry."
INDEX { recipientIndex }
 ::= { snmpNoticationRecipientTable 1 }
recipientIndex OBJECT-TYPE
SYNTAX       CmaDefaultTableIndexRange
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Unique system-assigned ID for this entry."
::= { snmpNotificationRecipientTableEntry 1 }

recipientIPAddressType OBJECT-TYPE
SYNTAX       InetAddressType
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "IP address type of the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 2 }

recipientIPAddress OBJECT-TYPE
SYNTAX       InetAddress
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "IP address of the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 3 }

recipientPort OBJECT-TYPE
SYNTAX       InetPortNumber
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "IP port number of the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 4 }

recipientTransportType OBJECT-TYPE
SYNTAX       SnmpTransportType
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Transport type for the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 5 }

recipientNotificationType OBJECT-TYPE
SYNTAX       SnmpNotificationType
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Notification type (trap or inform) for the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 6 }

recipientSnmpVersion OBJECT-TYPE
SYNTAX       SnmpVersionType
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "SNMP version of notifications for the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 7 }

recipientSecurityUser OBJECT-TYPE
SYNTAX       OCTET STRING (SIZE(0..255))
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "SNMP V3 security user name for the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 8 }

recipientAuthenticationType OBJECT-TYPE
SYNTAX       SnmpAuthenticationType
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION "SNMP V3 authentication type for the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 9 }

recipientEncryptionType OBJECT-TYPE
SYNTAX  SnmpEncryptionType
MAX-ACCESS read-only
STATUS   current
DESCRIPTION "SNMP V3 encryption type for the SNMP recipient."
::= { snmpNotificationRecipientTableEntry 10 }

-- END SNMP configuration

-- START CMA Server license configuration
CmaConfigLicenseFeatureTableEntry ::= SEQUENCE
{
  featureIndex          CmaDefaultTableIndexRange,
  featureLicense        FeatureLicense,
  enabled               TruthValue,
  licenseCount          Integer32,
  activatedDate         DateAndTime,
  expirationDate        DateAndTime
}

cmaConfigLicenseFeatureTableEntry OBJECT-TYPE
SYNTAX  CmaConfigLicenseFeatureTableEntry
MAX-ACCESS not-accessible
STATUS   current
DESCRIPTION "CMA License feature table entry."
INDEX    { featureIndex }
::= { cmaConfigLicenseFeatureTable 1 }

featureIndex OBJECT-TYPE
SYNTAX  CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS   current
DESCRIPTION "Feature index."
::= { cmaConfigLicenseFeatureTableEntry 1 }

featureLicense         OBJECT-TYPE
SYNTAX  FeatureLicense
MAX-ACCESS read-only
STATUS   current
DESCRIPTION "Licensed feature."
::= { cmaConfigLicenseFeatureTableEntry 2 }

FeatureLicense ::= TEXTUAL-CONVENTION
STATUS   current
DESCRIPTION "Licensed feature values."
SYNTAX    INTEGER
{  
  dmaIntegration(2),
  multiTenant(3),
  managementOfEndpointsAndServices(11),
  serviceProviderApi(22)
}

eranked OBJECT-TYPE
SYNTAX  TruthValue
MAX-ACCESS read-only
STATUS   current
DESCRIPTION "Is feature enabled."
DEFVAL    { false }
::= { cmaConfigLicenseFeatureTableEntry 3 }

licenseCount OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "License count. If the license feature does not have an associated license count then the
licenseCount will return -1 to indicate that the count is not applicable for this feature."
DEFVAL    { 0 }
::= { cmaConfigLicenseFeatureTableEntry 4 }

activatedDate OBJECT-TYPE
SYNTAX     DateAndTime
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Activated date of license. If there is no set date for the license activation then
1970-1-1,0:0:0.0 will be returned."
::= { cmaConfigLicenseFeatureTableEntry 5 }

expirationDate OBJECT-TYPE
SYNTAX     DateAndTime
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Expiration date of license. If there is not set date for the license expiration then
9999-12-31,0:0:0.0 will be returned."
::= { cmaConfigLicenseFeatureTableEntry 6 }

cmaConfigLicenseGroup OBJECT-GROUP
OBJECTS
{
cmaConfigLicenseSystemSerialNumber,
cmaConfigLicenseExpirationDays,
cmaConfigLicenseCmadLicenseReclaimationThreshold,
cmaConfigLicenseSupportedVersions,
cmaConfigLicenseServerType,
cmaConfigLicenseStatus,
featureIndex,
licenseCount,
enabled,
activatedDate,
expirationDate
}
STATUS current
DESCRIPTION "CMA license configuration conformance group."
::= { cmaConfigConformance 23 }

cmaConfigLicenseSystemSerialNumber OBJECT-TYPE
SYNTAX     OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "CMA license serial number."
::= { cmaConfigLicenses 1 }

cmaConfigLicenseExpirationDays OBJECT-TYPE
SYNTAX     Integer32 (0..90)
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Returns how many days left before it expired only if
the license will expire in 30 days, otherwise return -1."
::= { cmaConfigLicenses 2 }

cmaConfigLicenseCmadLicenseReclaimationThreshold OBJECT-TYPE
SYNTAX     Integer32 (0..90)
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of days of inactivity by a CMAD before its license is returned
to the available pool. Set to 0 to not reclaim CMAD licenses."
::= { cmaConfigLicenses 3 }

cmaConfigLicenseSupportedVersions OBJECT-TYPE
SYNTAX     OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Supported CMA versions."
::= { cmaConfigLicenses 4 }

cmaConfigLicenseServerType OBJECT-TYPE
SYNTAX     CmaConfigLicenseServerType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The type of the CMA server."
::= { cmaConfigLicenses 5 }

CmaConfigLicenseServerType ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "The type values of the CMA server.”
SYNTAX
{ primary(1),
  secondary(2)
}

cmaConfigLicenseStatus OBJECT-TYPE
SYNTAX     CmaConfigLicenseStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The status of the license."
::= { cmaConfigLicenses 6 }

CmaConfigLicenseStatus ::= TEXTUAL-CONVENTION
STATUS current
DESCRIPTION "The status values of the license.”
SYNTAX
{ active(1),
  inactive(2),
  expired(3)
}

cmaConfigLicenseFeatureTable OBJECT-TYPE
SYNTAX     SEQUENCE OF CmaConfigLicenseFeatureTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "License feature table.”
::= { cmaConfigLicenses 7 }
-- END CMA Server license configuration
-- START CMA Email Customization

cmaEmailCustomizationGroup  OBJECT-GROUP
  OBJECTS
  {
    cmaEmailCustomizationStart,
    cmaEmailCustomizationEnd
  }
  STATUS current
  DESCRIPTION "CMA Email Customization conformance group."
  ::= { cmaConfigConformance 24 }

    cmaEmailCustomizationStart OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0..650))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "CMA Email Customization - Beginning of the scheduling reminder email"
    ::= { cmaEmailCustomization 1 }

    cmaEmailCustomizationEnd OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0..650))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "CMA Email Customization - End of the scheduling reminder email"
    ::= { cmaEmailCustomization 2 }

-- END CMA Email Customization

-- START CMA CDR Archive Settings

cmaConfigCDRArchiveSettingsGroup  OBJECT-GROUP
  OBJECTS
  {
    cmaConfigDaysToKeepEndpointCDRs,
    cmaConfigCDRArchiveEnabled,
    cmaConfigCDRArchiveFirstDay,
    cmaConfigCDRArchiveUseSecureFTP,
    cmaConfigCDRArchiveFTPServer,
    cmaConfigCDRArchiveFTPPort,
    cmaConfigCDRArchiveUserName,
    cmaConfigCDRArchiveFPDDirectory
  }
  STATUS current
  DESCRIPTION "CMA CDR Archive Settings."
  ::= { cmaConfigConformance 25 }

    cmaConfigDaysToKeepEndpointCDRs OBJECT-TYPE
    SYNTAX       Integer32 (0..60)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "Number of days that Endpoint CDRs are retained on the CMA."
    ::= { cmaConfigCDRArchive 1 }

    cmaConfigCDRArchiveEnabled OBJECT-TYPE
    SYNTAX       TruthValue
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "Flag indicating whether to archive Endpoint CDRs to an external FTP server in CSV Format."
    ::= { cmaConfigCDRArchive 2 }
cmaConfigCDRArchiveFirstDay OBJECT-TYPE
SYNTAX    CmaConfigDayOfWeek
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "First day of weekly archive of Endpoint CDRs."
::= { cmaConfigCDRArchive 3 }

cmaConfigCDRArchiveUseSecureFTP OBJECT-TYPE
SYNTAX    TruthValue
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Use Secure FTP (SFTP) for archive of Endpoint CDRs."
::= { cmaConfigCDRArchive 4 }

cmaConfigCDRArchiveFTPServer OBJECT-TYPE
SYNTAX    OCTET STRING (SIZE(0..100))
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Hostname or IP Address of FTP server to use for archive of Endpoint CDRs."
::= { cmaConfigCDRArchive 5 }

cmaConfigCDRArchiveFTPPort OBJECT-TYPE
SYNTAX    Integer32 (1..65535)
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "FTP port of FTP server to use for archive of Endpoint CDRs."
::= { cmaConfigCDRArchive 6 }

cmaConfigCDRArchiveUserName OBJECT-TYPE
SYNTAX    OCTET STRING (SIZE(0..100))
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Username for the FTP server to use for archive of Endpoint CDRs."
::= { cmaConfigCDRArchive 7 }

cmaConfigCDRArchiveFTPDirectory OBJECT-TYPE
SYNTAX    OCTET STRING (SIZE(0..100))
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Directory on the FTP server to use for archive of Endpoint CDRs."
::= { cmaConfigCDRArchive 8 }

--cmaConfigLocalUserAccount Group

cmaConfigLocalUserAccountGroup OBJECT-GROUP
OBJECTS
{
    cmaLocalUserFailedLoginThreshold,
    cmaLocalUserFailedLoginWindow,
    cmaLocalUserAccountLockoutDuration,
    cmaLocalUserAccountThresholdAccount
}
STATUS current
DESCRIPTION "CMA Local User Account config conformance group."
::= { cmaConfigConformance 26 }

cmaLocalUserFailedLoginThreshold OBJECT-TYPE
SYNTAX    Integer32
MAX-ACCESS read-only
STATUS    current
DESCRIPTION "Number of failed logins allowed for a user."
::= {cmaConfigLocalUserAccount 1}

cmaLocalUserFailedLoginWindow OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Failed login window in hours for a particular user."
::= {cmaConfigLocalUserAccount 2}

cmaLocalUserAccountLockoutDuration OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "The account lockout duration (minutes) for user accounts which have exceeded the failed login threshold. If the lockout is indefinite and must be manually unlocked, then this will have a value of -1."
::= {cmaConfigLocalUserAccount 3}

cmaLocalUserAccountThresholdAccount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Customise Account Inactivity for the number of days"
::= {cmaConfigLocalUserAccount 4}

--End ConfigLocalUserAccount Group

--Start Local Password Requirement Configuration

CmaConfigLocalPasswordRequirementGroup OBJECT-GROUP
OBJECTS
{
cmaLocalPasswordMinLen,
cmaLocalPasswordMinChangedChar,
cmaLocalPasswordMinAgeCheck,
cmaLocalPasswordMinAge,
cmaLocalPasswordMaxAgeCheck,
cmaLocalPasswordMaxAge,
cmaLocalPasswordWarningIntervalCheck,
cmaLocalPasswordWarningInterval,
cmaLocalPasswordRejectPreviousCheck,
cmaLocalPasswordRejectPrevious,
cmaLocalPasswordIncludeLowerCase,
cmaLocalPasswordLowerCaseCount,
cmaLocalPasswordIncludeUpperCase,
cmaLocalPasswordUpperCaseCount,
cmaLocalPasswordIncludeNumbers,
cmaLocalPasswordNumbersCount,
cmaLocalPasswordIncludeSpecialChars,
cmaLocalPasswordSpecialCharsCount,
cmaLocalPasswordConsecutive,
cmaLocalPasswordConsecutiveCount
}
STATUS current
DESCRIPTION "CMA Local Password Requirement config conformance group."
::= {cmaConfigConformance 27}

cmaLocalPasswordMinLen OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Minimum Length of the Password."
 ::= { cmaConfigLocalPasswordRequirement  1 }

cmaLocalPasswordMinChangedChar   OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Minimum number of changed characters in the password."
 ::= { cmaConfigLocalPasswordRequirement  2 }

cmaLocalPasswordMinAgeCheck   OBJECT-TYPE
SYNTAX       TruthValue
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Check for the minimum age of LocalPassword."
 ::= { cmaConfigLocalPasswordRequirement  3 }

cmaLocalPasswordMinAge   OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Minimum Age of password allowed."
 ::= { cmaConfigLocalPasswordRequirement  4 }

cmaLocalPasswordMaxAgeCheck   OBJECT-TYPE
SYNTAX       TruthValue
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Check for the max age the password allowed."
 ::= { cmaConfigLocalPasswordRequirement  5 }

cmaLocalPasswordMaxAge   OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Max age of the password allowed."
 ::= { cmaConfigLocalPasswordRequirement  6 }

cmaLocalPasswordWarningIntervalCheck   OBJECT-TYPE
SYNTAX       TruthValue
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Check for password warning interval in days."
 ::= { cmaConfigLocalPasswordRequirement  7 }

cmaLocalPasswordWarningInterval   OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Password warning interval."
 ::= { cmaConfigLocalPasswordRequirement  8 }

cmaLocalPasswordRejectPreviousCheck   OBJECT-TYPE
SYNTAX       TruthValue
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION "Reject previous passwords checkbox ."
::= { cmaConfigLocalPasswordRequirement 9 }

cmaLocalPasswordRejectPrevious OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Reject previous passwords checkbox ."
::= { cmaConfigLocalPasswordRequirement 10 }

cmaLocalPasswordIncludeLowerCase OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Allow lower cases to be included in the password ."
::= { cmaConfigLocalPasswordRequirement 11 }

cmaLocalPasswordLowerCaseCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of lower case characters included ."
::= { cmaConfigLocalPasswordRequirement 12 }

cmaLocalPasswordIncludeUpperCase OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Include upper case in the password ."
::= { cmaConfigLocalPasswordRequirement 13 }

cmaLocalPasswordUpperCaseCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of upper case characters included ."
::= { cmaConfigLocalPasswordRequirement 14 }

cmaLocalPasswordIncludeNumbers OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Include numbers in the password ."
::= { cmaConfigLocalPasswordRequirement 15 }

cmaLocalPasswordNumbersCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of numbers allowed in the password ."
::= { cmaConfigLocalPasswordRequirement 16 }

cmaLocalPasswordIncludeSpecialChars OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Include special characters in the password ."
::= { cmaConfigLocalPasswordRequirement 17 }

cmaLocalPasswordSpecialCharsCount OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "number of special characters in the password."
::= { cmaConfigLocalPasswordRequirement 18 }

cmaLocalPasswordConsecutive   OBJECT-TYPE
SYNTAX       TruthValue
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Include consecutive repetition of characters."
::= { cmaConfigLocalPasswordRequirement 19 }

cmaLocalPasswordConsecutiveCount   OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "number of repetition of the same character in the password."
::= { cmaConfigLocalPasswordRequirement 20 }

--End Local Password Requirement Configuration

-- Status Group

-- START Connected User status

-- Status Group

-- Connected User status

cmaStatusUsersGroup  OBJECT-GROUP
OBJECTS
{
  connectedUserCount,
  connectedAdminUserCount,
  connectedOperatorUserCount,
  connectedSchedulerUserCount,
  connectedAuditorUserCount,
  connectedUserIndex,
  connectedUserName,
  connectedUserRole,
  connectedUserLoginTime
}
STATUS       current
DESCRIPTION  "CMA connected user status conformance group."
::= { cmaStatusConformance 1 }

connectedUserCount   OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS       current
DESCRIPTION  "Total number of connected CMA users."
::= { cmaStatusUsers 1 }

connectedAdminUserCount   OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS       current
DESCRIPTION  "Number of connected Administrator users."
::= { cmaStatusUsers 2 }
connectedOperatorUserCount   OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of connected Operator users."
::= { cmaStatusUsers 3 }

connectedSchedulerUserCount   OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of connected Scheduler users."
::= { cmaStatusUsers 4 }

connectedAuditorUserCount   OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of connected Scheduler users."
::= { cmaStatusUsers 5 }

-- Connected User table
ConnectedUserTableRange ::= Integer32 (1..255)
ConnectedUserTableEntry ::= SEQUENCE
{  
  connectedUserIndex   ConnectedUserTableRange,
  connectedUserName   OCTET STRING,
  connectedUserRole   OCTET STRING,
  connectedUserLoginTime  DateAndTime
}

connectedUserTable OBJECT-TYPE
SYNTAX        SEQUENCE OF ConnectedUserTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "Connected user table. Contains the names, roles, and login times
of the connected users."
::= { cmaStatusUsers 6 }

connectedUserTableEntry OBJECT-TYPE
SYNTAX        ConnectedUserTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "Connected user table entry."
INDEX   { connectedUserIndex }
::= { connectedUserTable 1 }

connectedUserIndex OBJECT-TYPE
SYNTAX      ConnectedUserTableRange
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "Unique system-assigned ID for this entry."
::= { connectedUserTableEntry 1 }

connectedUserName OBJECT-TYPE
SYNTAX      OCTET STRING (SIZE(0..255))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION "Name of the connected user."
::= { connectedUserTableEntry 2 }
connectedUserRole OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Role of the connected user."
::= { connectedUserTableEntry 3 }

c.connectedUserLoginTime OBJECT-TYPE
SYNTAX DateAndTime
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Login time of the connected user."
::= { connectedUserTableEntry 4 }

-- END Connected User status

-- START CMA Server license status


cmaStatusLicenseGroup OBJECT-GROUP
OBJECTS
{
cmaLicenseSeatCount,
cmaLicenseSeatsInUse
}
STATUS current
DESCRIPTION "CMA license status conformance group."
::= { cmaStatusLicenses 1 }

cmaLicenseSeatCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of CMAD seats in the license."
::= { cmaStatusLicenses 1 }

cmaLicenseSeatsInUse OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of licensed seats in use."
::= { cmaStatusLicenses 2 }

-- END CMA Server license status

-- START scheduled endpoint management status


cmaStatusEndpointManagementGroup OBJECT-GROUP
OBJECTS
{
cmaEpManagementPendingSoftUpdates,
cmaEpManagementInProgressSoftUpdates,
cmaEpManagementSuccessfulSoftUpdates,
cmaEpManagementPendingProvisioning,
cmaEpManagementInProgressProvisioning,
cmaEpManagementSuccessfulProvisioning,
cmaEpManagementFailedProvisioning
}
STATUS current
DESCRIPTION "CMA endpoint management status conformance group."
::= { cmaStatusConformance 6 }

cmaEpManagementInProgressSoftUpdates OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of in-progress endpoint soft updates."
::= { cmaStatusEndpointManagement 1 }

cmaEpManagementInProgressProvisioning OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of in-progress endpoint provisioning jobs."
::= { cmaStatusEndpointManagement 2 }

--cmaEpManagementPendingSoftUpdates OBJECT-TYPE
-- SYNTAX Integer32
-- MAX-ACCESS read-only
-- STATUS current
-- DESCRIPTION "Number of pending endpoint soft updates."
-- ::= { cmaStatusEndpointManagement 1 }

--cmaEpManagementSuccessfulSoftUpdates OBJECT-TYPE
-- SYNTAX Integer32
-- MAX-ACCESS read-only
-- STATUS current
-- DESCRIPTION "Number of successful soft updates."
-- ::= { cmaStatusEndpointManagement 4 }

--cmaEpManagementFailedSoftUpdates OBJECT-TYPE
-- SYNTAX Integer32
-- MAX-ACCESS read-only
-- STATUS current
-- DESCRIPTION "Number of failed soft updates."
-- ::= { cmaStatusEndpointManagement 5 }

--cmaEpManagementPendingProvisioning OBJECT-TYPE
-- SYNTAX Integer32
-- MAX-ACCESS read-only
-- STATUS current
-- DESCRIPTION "Number of pending endpoint provisioning jobs."
-- ::= { cmaStatusEndpointManagement 6 }

--cmaEpManagementSuccessfulProvisioning OBJECT-TYPE
-- SYNTAX Integer32
-- MAX-ACCESS read-only
-- STATUS current
-- DESCRIPTION "Number of successful provisioning jobs."
-- ::= { cmaStatusEndpointManagement 8 }

--cmaEpManagementFailedProvisioning OBJECT-TYPE
-- SYNTAX Integer32
-- MAX-ACCESS read-only
-- STATUS current
-- DESCRIPTION "Number of failed provisioning jobs."
-- ::= { cmaStatusEndpointManagement 9 }

-- END scheduled endpoint management status
-- START MCU status

cmaStatusDeviceGroup OBJECT-GROUP
  OBJECTS
  {
    cmaMcuCount,
    cmaMcuCountWithWarnings,
    cmaMcuCountWithErrors,
    cmaMcuIndex,
    cmaMcuName,
    cmaMcuType,
    cmaMcuInetAddressType,
    cmaMcuInetAddress,
    cmaMcuStatus,
    cmaMcuConferenceCount,
    cmaMcuAudioPortsUsed,
    cmaMcuVideoPortsUsed,
    cmaEndpointCount,
    cmaEndpointCountWithAlerts,
    cmaEndpointCountWithHelpRequests,
    cmaEndpointCountOnline,
    cmaEndpointCountOffline,
    cmaEndpointCountInCall,
    cmaEndpointIndex,
    cmaEndpointId,
    cmaEndpointOwner,
    cmaEndpointIsdnVideoNumber,
    cmaEndpointSoftwareVersion,
    cmaEndpointType,
    cmaEndpointInetAddressType,
    cmaEndpointInetAddress,
    cmaEndpointStatus,
    cmaEndpointInCall,
    cmaEndpointGatekeeperRegStatus,
    cmaEndpointGabRegStatus,
    cmaEndpointPresenceRegStatus,
    cmaEndpointSipRegStatus,
    cmaEndpointManagementStatus,
    cmaEndpointErrorCount,
    cmaEndpointErrors,
    cmaEndpointWarningCount,
    cmaEndpointWarnings,
    cmaEndpointHelpRequest,
    cmaEndpointSerialNumber,
    cmaEndpointAvailableToSchedule,
    cmaEndpointRegisteredAliases,
    cmaEndpointSipUri,
    cmaEndpointGatekeeperAddress,
    cmaEndpointSipServerAddress,
    cmaVbpCount,
    cmaVbpIndex,
    cmaVbpModel,
    cmaVbpName,
    cmaVbpLanInetAddressType,
    cmaVbpLanInetAddress,
    cmaVbpWanInetAddressType,
    cmaVbpWanInetAddress,
    cmaDmaCount,
    cmaDmaIndex,
    cmaDmaName,
    cmaDmaInetAddressType,
cmaDmaInetAddress,
cmaDmaStatus,
cmaDmaIsCallServer,
cmaDmaIsConferenceManager,
cmaDmaH323Enabled,
cmaDmaSipEnabled,
cmaDmaSiteTopologyIntegrated,
cmaEndpointExchangeStatus,
cmaEndpointPeripheralIconState,
cmaEndpointPeripheralStatus,
cmaPeripheralIndex,
cmaPeripheralPairedStatus,
cmaPeripheralAlertState,
cmaPeripheralPairedName,
cmaPeripheralDeviceType,
cmaPeripheralSerialNumber,
cmaPeripheralInetAddress,
cmaPeripheralInetAddressType,
cmaPeripheralHardwareVersion,
cmaPeripheralSoftwareVersion,
cmaPeripheralCount,
cmaEndpointExchangeStatus,
cmaEndpointPeripheralIconState,
cmaEndpointPeripheralStatus,
cmaPeripheralIndex,
cmaPeripheralPairedStatus,
cmaPeripheralAlertState,
cmaPeripheralPairedName,
cmaPeripheralDeviceType,
cmaPeripheralSerialNumber,
cmaPeripheralInetAddress,
cmaPeripheralInetAddressType,
cmaPeripheralHardwareVersion,
cmaPeripheralSoftwareVersion,
cmaPeripheralCount,
cmaPeripheralIndex,
cmaPeripheralPairedStatus,
cmaPeripheralAlertState,
cmaPeripheralPairedName,
cmaPeripheralDeviceType,
cmaPeripheralSerialNumber,
cmaPeripheralInetAddress,
cmaPeripheralInetAddressType,
cmaPeripheralHardwareVersion,
cmaPeripheralSoftwareVersion,
cmaPeripheralCount,
cmaEndpointExchangeStatus,
cmaEndpointPeripheralIconState,
cmaEndpointPeripheralStatus,
cmaPeripheralIndex,
cmaPeripheralPairedStatus,
cmaPeripheralAlertState,
cmaPeripheralPairedName,
cmaPeripheralDeviceType,
cmaPeripheralSerialNumber,
cmaPeripheralInetAddress,
cmaPeripheralInetAddressType,
cmaPeripheralHardwareVersion,
cmaPeripheralSoftwareVersion,
cmaPeripheralCount,
cmaEndpointExchangeStatus,
cmaEndpointPeripheralIconState,
cmaEndpointPeripheralStatus,
cmaPeripheralIndex,
cmaPeripheralPairedStatus,
cmaPeripheralAlertState,
cmaPeripheralPairedName,
cmaPeripheralDeviceType,
cmaPeripheralSerialNumber,
cmaPeripheralInetAddress,
cmaPeripheralInetAddressType,
cmaPeripheralHardwareVersion,
cmaPeripheralSoftwareVersion,
cmaPeripheralCount,
cmaEndpointExchangeStatus,
cmaEndpointPeripheralIconState,
cmaEndpointPeripheralStatus,
cmaPeripheralIndex,
cmaPeripheralPairedStatus,
cmaPeripheralAlertState,
cmaPeripheralPairedName,
cmaPeripheralDeviceType,
CmaMcuStatusTableEntry ::= SEQUENCE
{
  cmaMcuIndex          CmaDefaultTableIndexRange,
  cmaMcuName           OCTET STRING,
  cmaMcuType           CmaMcuType,
  cmaMcuInetAddressType InetAddressType,
  cmaMcuInetAddress    InetAddress,
  cmaMcuStatus         CmaDeviceStatus,
  cmaMcuConferenceCount Integer32, -- Number of active conferences
  cmaMcuAudioPortsUsed Integer32,  -- % of audio ports in use
  cmaMcuVideoPortsUsed Integer32    -- % of video ports in use
}

cmaMcuStatusTable OBJECT-TYPE
SYNTAX        SEQUENCE OF CmaMcuStatusTableEntry
MAX-ACCESS   not-accessible
STATUS       current
DESCRIPTION  "MCU status table. Contains identification, status,
              and usage information for MCUs."
::= { cmaStatusDeviceMCU 4 }

cmaMcuStatusTableEntry OBJECT-TYPE
SYNTAX        CmaMcuStatusTableEntry
MAX-ACCESS   not-accessible
STATUS       current
DESCRIPTION  "MCU status table entry."
INDEX        { cmaMcuIndex }
::= { cmaMcuStatusTable 1 }

cmaMcuIndex OBJECT-TYPE
SYNTAX       CmaDefaultTableIndexRange
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Unique system-assigned ID for this entry."
::= { cmaMcuStatusTableEntry 1 }

cmaMcuName OBJECT-TYPE
SYNTAX       OCTET STRING (SIZE(1..255))
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Name of the MCU."
::= { cmaMcuStatusTableEntry 2 }

cmaMcuType OBJECT-TYPE
SYNTAX       CmaMcuType
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "MCU type."
::= { cmaMcuStatusTableEntry 3 }

cmaMcuInetAddressType OBJECT-TYPE
SYNTAX       InetAddressType
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "IP address type of the MCU."
::= { cmaMcuStatusTableEntry 4 }

cmaMcuInetAddress OBJECT-TYPE
SYNTAX       InetAddress
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "IP address of the MCU."
::= { cmaMcuStatusTableEntry 5 }

-- END MCU status

-- START endpoint status

cmaEndpointCount OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Total number of endpoints known to the CMA server."
::= { cmaStatusDeviceEndpoint 1 }

cmaEndpointCountWithAlerts OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Number of endpoints with alert conditions."
::= { cmaStatusDeviceEndpoint 2 }

cmaEndpointCountWithHelpRequests OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Number of endpoints with help requests."
::= { cmaStatusDeviceEndpoint 3 }

cmaEndpointCountOnline OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only

-- END endpoint status
MIB Reference

STATUS current
DESCRIPTION "Number of endpoints that are on line."
::= { cmaStatusDeviceEndpoint 4 }
cmaEndpointCountOffline OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of endpoints that are off line."
::= { cmaStatusDeviceEndpoint 5 }
cmaEndpointCountInCall OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of endpoints that are in a call."
::= { cmaStatusDeviceEndpoint 6 }
CmaEndpointStatusTableEntry ::= SEQUENCE
{
cmaEndpointIndex CmaDefaultTableIndexRange,
cmaEndpointType CmaEndpointType,
cmaEndpointId Integer32,
cmaEndpointOwner OCTET STRING,
cmaEndpointIsdnVideoNumber OCTET STRING,
cmaEndpointInetAddressType InetAddressType,
cmaEndpointInetAddress InetAddress,
cmaEndpointStatus CmaDeviceStatus, -- online or offline
cmaEndpointInCall TruthValue,
cmaEndpointGatekeeperRegStatus CmaDeviceRegistrationStatus,
cmaEndpointGabRegStatus CmaDeviceRegistrationStatus,
cmaEndpointPresenceRegStatus CmaDeviceRegistrationStatus,
cmaEndpointSipRegStatus CmaDeviceRegistrationStatus,
cmaEndpointManagementStatus CmaDeviceManagementStatus,
cmaEndpointErrorCount Integer32,
cmaEndpointErrors OCTET STRING,
cmaEndpointWarningCount Integer32,
cmaEndpointWarnings OCTET STRING,
cmaEndpointHelpRequest TruthValue,
cmaEndpointExchangeStatus CmaDeviceRegistrationStatus,
cmaEndpointPeripheralIconState CmaPeripheralIconState,
cmaEndpointPeripheralStatus CmaPeripheralPairingStatus,
cmaEndpointSoftwareVersion OCTET STRING,
cmaEndpointSerialNumber OCTET STRING,
cmaEndpointAvailableToSchedule TruthValue,
cmaEndpointRegisteredAliases OCTET STRING,
cmaEndpointSipUri OCTET STRING,
cmaEndpointGatekeeperAddress InetAddress,
cmaEndpointSipServerAddress InetAddress
}
cmaEndpointStatusTable OBJECT-TYPE
SYNTAX SEQUENCE OF CmaEndpointStatusTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "Endpoint status table. Contains identification and status information for endpoints."
::= { cmaStatusDeviceEndpoint 7 }
cmaEndpointStatusTableEntry OBJECT-TYPE
SYNTAX CmaEndpointStatusTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "Endpoint status table entry."
INDEX { cmaEndpointIndex }
::= { cmaEndpointStatusTable 1 }

cmaEndpointIndex OBJECT-TYPE
SYNTAX CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Unique system-assigned ID for this entry."
::= { cmaEndpointStatusTableEntry 1 }

cmaEndpointType OBJECT-TYPE
SYNTAX CmaEndpointType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Type of endpoint."
::= { cmaEndpointStatusTableEntry 2 }

cmaEndpointId OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Id of endpoint."
::= { cmaEndpointStatusTableEntry 3 }

cmaEndpointOwner OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Endpoint Owner."
::= { cmaEndpointStatusTableEntry 4 }

cmaEndpointIsdnVideoNumber OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Endpoint Isdn Video Number."
::= { cmaEndpointStatusTableEntry 5 }

cmaEndpointInetAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address type of the endpoint."
::= { cmaEndpointStatusTableEntry 6 }

cmaEndpointInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the endpoint."
::= { cmaEndpointStatusTableEntry 7 }

cmaEndpointStatus OBJECT-TYPE
SYNTAX CmaDeviceStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Status of the endpoint."
::= { cmaEndpointStatusTableEntry 8 }

cmaEndpointInCall OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the endpoint is in a call."
::= { cmaEndpointStatusTableEntry 9 }

cmaEndpointGatekeeperRegStatus OBJECT-TYPE
SYNTAX CmaDeviceRegistrationStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Gatekeeper registration status of the endpoint."
::= { cmaEndpointStatusTableEntry 10 }

cmaEndpointGabRegStatus OBJECT-TYPE
SYNTAX CmaDeviceRegistrationStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "GAB registration status of the endpoint."
::= { cmaEndpointStatusTableEntry 11 }

cmaEndpointPresenceRegStatus OBJECT-TYPE
SYNTAX CmaDeviceRegistrationStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Presence registration status of the endpoint."
::= { cmaEndpointStatusTableEntry 12 }

cmaEndpointSipRegStatus OBJECT-TYPE
SYNTAX CmaDeviceRegistrationStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "SIP registration status of the endpoint."
::= { cmaEndpointStatusTableEntry 13 }

cmaEndpointManagementStatus OBJECT-TYPE
SYNTAX CmaDeviceManagementStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Management status of the endpoint."
::= { cmaEndpointStatusTableEntry 14 }

cmaEndpointErrorCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of errors on the endpoint."
::= { cmaEndpointStatusTableEntry 15 }

cmaEndpointErrors OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "List of the errors on the endpoint, separated by new-line characters."
::= { cmaEndpointStatusTableEntry 16 }
cmaEndpointWarningCount OBJECT-TYPE
SYNTAX     Integer32
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Number of warnings on the endpoint."
::= { cmaEndpointStatusTableEntry 17 }

cmaEndpointWarnings OBJECT-TYPE
SYNTAX     OCTET STRING
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "List of the warnings on the endpoint, separated by new-line characters."
::= { cmaEndpointStatusTableEntry 18 }

cmaEndpointHelpRequest OBJECT-TYPE
SYNTAX     TruthValue
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Flag indicating whether there is a help request on the endpoint."
::= { cmaEndpointStatusTableEntry 19 }

cmaEndpointExchangeStatus OBJECT-TYPE
SYNTAX     CmaDeviceRegistrationStatus
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Exchange server status of user associated with the endpoint."
::= { cmaEndpointStatusTableEntry 20 }

cmaEndpointPeripheralIconState OBJECT-TYPE
SYNTAX     CmaPeripheralIconState
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Peripheral icon state for this endpoint."
::= { cmaEndpointStatusTableEntry 21 }

cmaEndpointPeripheralStatus OBJECT-TYPE
SYNTAX     CmaPeripheralPairingStatus
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Peripheral status for this endpoint."
::= { cmaEndpointStatusTableEntry 22 }

cmaEndpointSoftwareVersion OBJECT-TYPE
SYNTAX     OCTET STRING
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Software Version running on this endpoint."
::= { cmaEndpointStatusTableEntry 23 }

cmaEndpointSerialNumber OBJECT-TYPE
SYNTAX     OCTET STRING
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Serial Number of this endpoint."
::= { cmaEndpointStatusTableEntry 24 }

cmaEndpointAvailableToSchedule OBJECT-TYPE
SYNTAX     TruthValue
MAX-ACCESS read-only
STATUS     current
DESCRIPTION "Flag indicating whether the endpoint is available to schedule."
::= { cmaEndpointStatusTableEntry 25 }
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   " Returns True if the Endpoint id available."
::= { cmaEndpointStatusTableEntry 25}

cmaEndpointRegisteredAliases     OBJECT-TYPE
SYNTAX        OCTET STRING
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Comma seperated list of gatekeeper registered aliases for this endpoint."
::= { cmaEndpointStatusTableEntry 26}

cmaEndpointSipUri          OBJECT-TYPE
SYNTAX        OCTET STRING
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "SipUri associated with this endpoint."
::= { cmaEndpointStatusTableEntry 27}

cmaEndpointGatekeeperAddress    OBJECT-TYPE
SYNTAX        InetAddress
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Host or IP address of the H.323 Gatekeeper for the endpoint."
::= { cmaEndpointStatusTableEntry 28}

cmaEndpointSipServerAddress     OBJECT-TYPE
SYNTAX        InetAddress
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Host or IP address of the SIP Server for the endpoint."
::= { cmaEndpointStatusTableEntry 29}

-- END endpoint status

-- START VBP status

cmaVbpCount OBJECT-TYPE
SYNTAX       Integer32
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Number of VBPs known to the CMA server."
::= { cmaStatusDeviceVBP 1 }

CmaVbpStatusTableEntry ::= SEQUENCE
{  
cmaVbpIndex                          CmaDefaultTableIndexRange,
cmaVbpModel                          CmaVbpModel1,
cmaVbpName                           OCTET STRING,
cmaVbpLanInetAddressType   InetAddressType,
cmaVbpLanInetAddress         InetAddress,
cmaVbpWanInetAddressType   InetAddressType,
cmaVbpWanInetAddress       InetAddress
}

CmaVbpStatusTable     OBJECT-TYPE
SYNTAX        SEQUENCE OF CmaVbpStatusTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "VBP status table. Contains information about Polycom Video Border Proxy devices."
::= { cmaStatusDeviceVBP 2 }

cmaVbpStatusTableEntry OBJECT-TYPE
SYNTAX CmaVbpStatusTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "VBP status table entry."
INDEX { cmaVbpIndex }
 ::= { cmaVbpStatusTable 1 }

cmaVbpIndex OBJECT-TYPE
SYNTAX CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Unique system-assigned ID for this entry."
 ::= { cmaVbpStatusTableEntry 1 }

cmaVbpModel OBJECT-TYPE
SYNTAX CmaVbpModel
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Model of the VBP device."
 ::= { cmaVbpStatusTableEntry 2 }

cmaVbpName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the VBP device."
 ::= { cmaVbpStatusTableEntry 3 }

cmaVbpLanInetAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "LAN IP address type of the VBP device."
 ::= { cmaVbpStatusTableEntry 4 }

cmaVbpLanInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "LAN IP address of the VBP device."
 ::= { cmaVbpStatusTableEntry 5 }

cmaVbpWanInetAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "WAN IP address type of the VBP device."
 ::= { cmaVbpStatusTableEntry 6 }

cmaVbpWanInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "WAN IP address of the VBP device."
 ::= { cmaVbpStatusTableEntry 7 }

-- END VBP status
-- START DMA status

cmaDmaCount OBJECT-TYPE
   SYNTAX Integer32
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION "Number of DMA systems known to the CMA server."
   ::= { cmaStatusDeviceDMA 1 }

CmaDmaStatusTableEntry ::= SEQUENCE
{
   cmaDmaIndex CmaDefaultTableIndexRange,
   cmaDmaName OCTET STRING,
   cmaDmaInetAddressType InetAddressType,
   cmaDmaInetAddress InetAddress,
   cmaDmaStatus CmaDeviceStatus,
   cmaDmaIsCallServer TruthValue,
   cmaDmaIsConferenceManager TruthValue,
   cmaDmaH323Enabled TruthValue,
   cmaDmaSipEnabled TruthValue,
   cmaDmaSiteTopologyIntegrated TruthValue
}

cmaDmaStatusTable OBJECT-TYPE
   SYNTAX SEQUENCE OF CmaDmaStatusTableEntry
   MAX-ACCESS not-accessible
   STATUS current
   DESCRIPTION "DMA status table. Contains information about DMA systems."
   ::= { cmaStatusDeviceDMA 2 }

CmaDmaStatusTableEntry OBJECT-TYPE
   SYNTAX CmaDmaStatusTableEntry
   MAX-ACCESS not-accessible
   STATUS current
   DESCRIPTION "DMA status table entry."
   INDEX { cmaDmaIndex }
   ::= { cmaDmaStatusTable 1 }

cmaDmaIndex OBJECT-TYPE
   SYNTAX CmaDefaultTableIndexRange
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION "Unique system-assigned ID for this entry."
   ::= { cmaDmaStatusTableEntry 1 }

cmaDmaName OBJECT-TYPE
   SYNTAX OCTET STRING (SIZE(1..255))
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION "Name of the DMA system."
   ::= { cmaDmaStatusTableEntry 2 }

cmaDmaInetAddressType OBJECT-TYPE
   SYNTAX InetAddressType
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION "Host/IP address type of the DMA system."
   ::= { cmaDmaStatusTableEntry 3 }
cmaDmaInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Host name or IP address of the DMA system."
::= { cmaDmaStatusTableEntry 4 }

cmaDmaStatus OBJECT-TYPE
SYNTAX CmaDeviceStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Current status of the DMA system."
::= { cmaDmaStatusTableEntry 5 }

cmaDmaIsCallServer OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating if the DMA is configured to be the Call Server for the system."
::= { cmaDmaStatusTableEntry 6 }

cmaDmaIsConferenceManager OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating if the DMA is configured to be the conference manager for the system for anytime and pooled conferences."
::= { cmaDmaStatusTableEntry 7 }

cmaDmaH323Enabled OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating if the DMA has H.323 signalling enabled."
::= { cmaDmaStatusTableEntry 8 }

cmaDmaSipEnabled OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating if the DMA has SIP signalling enabled."
::= { cmaDmaStatusTableEntry 9 }

cmaDmaSiteTopologyIntegrated OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating if the DMA is integrated with the XMA for site topology."
::= { cmaDmaStatusTableEntry 10 }

-- END DMA status

-- START Peripheral status

cmaPeripheralCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of peripherals known to the CMA server."
::= {cmaStatusDevicePeripherals 1 }

CmaPeripheralStatusTableEntry ::= SEQUENCE
{
cmaPeripheralIndex                      CmaDefaultTableIndexRange,  
cmaPeripheralPairedStatus               CmaPeripheralPairingStatus,    
cmaPeripheralAlertState                 CmaPeripheralAlertState,            
cmaPeripheralPairedName                 OCTET STRING,                
cmaPeripheralDeviceType                 CmaEndpointType,                  
cmaPeripheralSerialNumber               OCTET STRING,                  
cmaPeripheralInetAddress                InetAddress,                   
cmaPeripheralInetAddressType            InetAddressType,                
cmaPeripheralHardwareVersion            OCTET STRING,                   
cmaPeripheralSoftwareVersion            OCTET STRING
}

cmaPeripheralStatusTable      OBJECT-TYPE
SYNTAX        SEQUENCE OF CmaPeripheralStatusTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "Peripheral status table. Contains information
about Peripherals."
::= {cmaStatusDevicePeripherals 2 }

cmaPeripheralStatusTableEntry      OBJECT-TYPE
SYNTAX        CmaPeripheralStatusTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "DMA status table entry."
INDEX         { cmaPeripheralIndex }
::= {cmaPeripheralStatusTable 1}

cmaPeripheralIndex         OBJECT-TYPE
SYNTAX        CmaDefaultTableIndexRange
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Unique system-assigned ID for this entry."
::= {cmaPeripheralStatusTableEntry 1 }

cmaPeripheralPairedStatus         OBJECT-TYPE
SYNTAX        CmaPeripheralPairingStatus
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Current pairing status for the peripheral."
::= {cmaPeripheralStatusTableEntry 2 }

cmaPeripheralAlertState         OBJECT-TYPE
SYNTAX        CmaPeripheralAlertState
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Current error state for the peripheral."
::= {cmaPeripheralStatusTableEntry 3 }

cmaPeripheralPairedName         OBJECT-TYPE
SYNTAX        OCTET STRING (SIZE(1..255))
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Name of the paired HDX."
::= {cmaPeripheralStatusTableEntry 4 }

Polycom, Inc. 617
cmaPeripheralDeviceType OBJECT-TYPE
SYNTAX CmaEndpointType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Device type for this peripheral."
::= { cmaPeripheralStatusTableEntry 5 }

cmaPeripheralSerialNumber OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Serial number for this peripheral."
::= { cmaPeripheralStatusTableEntry 6 }

cmaPeripheralInetAddress OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the peripheral."
::= { cmaPeripheralStatusTableEntry 7 }

cmaPeripheralInetAddressType OBJECT-TYPE
SYNTAX InetSocketAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Inet address type for this peripheral."
::= { cmaPeripheralStatusTableEntry 8 }

cmaPeripheralHardwareVersion OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Hardware version for this peripheral."
::= { cmaPeripheralStatusTableEntry 9 }

cmaPeripheralSoftwareVersion OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Software version for this peripheral."
::= { cmaPeripheralStatusTableEntry 10 }

-- END Peripheral status

-- START SAM status

cmaSamCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total number of SAMs known to the CMA server."
::= { cmaStatusDeviceSAM 1 }

CmaSamStatusTableEntry ::= SEQUENCE
{ cmaSamIndex CmaDefaultTableIndexRange, cmaSamName OCTET STRING, cmaSamStatus CmaDeviceStatus, cmaSamProviderSiteAddress InetSocketAddress, cmaSamSiteName OCTET STRING }
cmaSamStatusTable OBJECT-TYPE
SYNTAX SEQUENCE OF CmaSamStatusTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "SAM status table. Contains status, name, provider-side IP and site information for SAMs."
::= { cmaStatusDeviceSAM 2 }

cmaSamStatusTableEntry OBJECT-TYPE
SYNTAX CmaSamStatusTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "SAM status table entry."
INDEX { cmaSamIndex }
::= { cmaSamStatusTable 1 }

cmaSamIndex OBJECT-TYPE
SYNTAX CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Unique system-assigned ID for this entry."
::= { cmaSamStatusTableEntry 1 }

cmaSamName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the SAM."
::= { cmaSamStatusTableEntry 2 }

cmaSamStatus OBJECT-TYPE
SYNTAX CmaDeviceStatus
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Status of the SAM."
::= { cmaSamStatusTableEntry 3 }

cmaSamProviderSideAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Provider side IP address of the SAM."
::= { cmaSamStatusTableEntry 4 }

cmaSamSiteName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Site Name of the SAM."
::= { cmaSamStatusTableEntry 5 }

-- END SAM status

-- START SBC status

cmaSbcCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of SBCs known to the CMA server."
::= { cmaStatusDeviceSBC 1 }

CmaSbcStatusTableEntry ::= SEQUENCE  
{
  cmaSbcIndex                     CmaDefaultTableIndexRange,
  cmaSbcName                      OCTET STRING,
  cmaSbcLanInetAddressType       InetAddressType,
  cmaSbcLanInetAddress          InetAddress,
  cmaSbcWanInetAddressType       InetAddressType,
  cmaSbcWanInetAddress          InetAddress
}

CmaSbcStatusTable OBJECT-TYPE
SYNTAX        SEQUENCE OF CmaSbcStatusTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "SBC status table. Contains information about Polycom Video Border Proxy devices."
::= { cmaStatusDeviceSBC 2 }

CmaSbcStatusTableEntry OBJECT-TYPE
SYNTAX        CmaSbcStatusTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "SBC status table entry."
INDEX         { cmaSbcIndex }
::= { cmaSbcStatusTable 1 }

CmaSbcIndex OBJECT-TYPE
SYNTAX        CmaDefaultTableIndexRange
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Unique system-assigned ID for this entry."
::= { cmaSbcStatusTableEntry 1 }

CmaSbcName OBJECT-TYPE
SYNTAX        OCTET STRING (SIZE(1..255))
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Name of the SBC device."
::= { cmaSbcStatusTableEntry 3 }

CmaSbcLanInetAddressType OBJECT-TYPE
SYNTAX        InetAddressType
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "LAN IP address type of the SBC device."
::= { cmaSbcStatusTableEntry 4 }

CmaSbcLanInetAddress OBJECT-TYPE
SYNTAX        InetAddress
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "LAN IP address of the SBC device."
::= { cmaSbcStatusTableEntry 5 }

CmaSbcWanInetAddressType OBJECT-TYPE
SYNTAX        InetAddressType
MAX-ACCESS    read-only

### SBC status

**cmaSbcWanInetAddress** **OBJECT-TYPE**
- **SYNTAX**: InetAddress
- **MAX-ACCESS**: read-only
- **STATUS**: current
- **DESCRIPTION**: “WAN IP address of the SBC device.”

```plaintext
cmaSbcWanInetAddress ::= { cmaSbcStatusTableEntry 7 }
```

**START Conference summary**

**cmaStatusConferenceGroup** **OBJECT-GROUP**

- **OBJECTS**
  ```plaintext
cmaConfSummaryCompletedScheduledCount, cmaConfSummaryActiveScheduledCount, cmaConfSummaryFutureScheduledCount, cmaConfSummaryCompletedAdhocCount, cmaConfSummaryActiveAdhocCount, cmaActiveConferenceCount, cmaConferenceIndex, cmaConferenceName, cmaConferenceScheduleId, cmaConferenceType, cmaConferenceIsScheduled, cmaConferenceIsRecurring, cmaConferenceStartTime, cmaConferenceOwner, cmaConferenceStatus, cmaConferenceTotalParticipants, cmaConferenceConnectedParticipants, cmaConferenceIsCascaded, cmaConferenceMcu, cmaConferenceAvgParticipantAudioQOE, cmaConferenceAvgParticipantVideoQOE, cmaConferenceAvgParticipantContentQOE, cmaConferenceMinParticipantAudioQOE, cmaConferenceMinParticipantVideoQOE, cmaConferenceMinParticipantContentQOE
```

**STATUS**: current
- **DESCRIPTION**: “CMA conference status conformance group.”

```plaintext
cmaStatusConferenceSummary 8 } `cmaStatusConformance 8 }
```

**cmaConfSummaryCompletedScheduledCount** **OBJECT-TYPE**
- **SYNTAX**: Integer32
- **MAX-ACCESS**: read-only
- **STATUS**: current
- **DESCRIPTION**: “Number of completed scheduled conferences since midnight.”

```plaintext
cmaConfSummaryCompletedScheduledCount ::= { cmaStatusConferenceSummary 1 }
```

**cmaConfSummaryActiveScheduledCount** **OBJECT-TYPE**
- **SYNTAX**: Integer32
- **MAX-ACCESS**: read-only
- **STATUS**: current
- **DESCRIPTION**: “Number of active scheduled conferences.”

```plaintext
cmaConfSummaryActiveScheduledCount ::= { cmaStatusConferenceSummary 1 }
```
::= { cmaStatusConferenceSummary 2 }

cmaConfSummaryFutureScheduledCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of future scheduled conferences for today (i.e., until midnight of the current day)."
::= { cmaStatusConferenceSummary 3 }

cmaConfSummaryCompletedAdhocCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of completed ad hoc conferences since midnight."
::= { cmaStatusConferenceSummary 4 }

cmaConfSummaryActiveAdhocCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of active ad hoc conferences."
::= { cmaStatusConferenceSummary 5 }

-- END Conference summary

-- START Conference status

::= { cmaStatusConferencesOngoing 1 }

CmaActiveConferenceTableEntry ::= SEQUENCE
{
    cmaConferenceIndex CmaDefaultTableIndexRange,
    cmaConferenceName OCTET STRING,
    cmaConferenceScheduleId OCTET STRING,
    cmaConferenceType CmaConferenceType,
    cmaConferenceIsScheduled TruthValue,
    cmaConferenceIsRecurring TruthValue,
    cmaConferenceStartTime DateAndTime,
    cmaConferenceOwner OCTET STRING,
    cmaConferenceStatus CmaConferenceStatus,
    cmaConferenceTotalParticipants Integer32,
    cmaConferenceConnectedParticipants Integer32,
    cmaConferenceIsCascaded TruthValue,
    cmaConferenceMcu OCTET STRING,
    cmaConferenceAvgParticipantAudioQOE Integer32,
    cmaConferenceAvgParticipantVideoQOE Integer32,
    cmaConferenceAvgParticipantContentQOE Integer32,
    cmaConferenceMinParticipantAudioQOE Integer32,
    cmaConferenceMinParticipantVideoQOE Integer32,
    cmaConferenceMinParticipantContentQOE Integer32
}

CmaActiveConferenceTable OBJECT-TYPE
SYNTAX SEQUENCE OF CmaActiveConferenceTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "Active conference table. Contains the available information for all active conferences."
::= { cmaStatusConferencesOngoing 2 }

cmaActiveConferenceTableEntry OBJECT-TYPE
SYNTAX CmaActiveConferenceTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION "Active conference table entry."
INDEX { cmaConferenceIndex }
::= { cmaActiveConferenceTable 1 }

cmaConferenceIndex OBJECT-TYPE
SYNTAX CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Unique system-assigned ID for this entry."
::= { cmaActiveConferenceTableEntry 1 }

cmaConferenceName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the conference."
::= { cmaActiveConferenceTableEntry 2 }

cmaConferenceScheduleId OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Scheduling ID of the conference."
::= { cmaActiveConferenceTableEntry 3 }

cmaConferenceType OBJECT-TYPE
SYNTAX CmaConferenceType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Type (audio-only or video) of the conference."
::= { cmaActiveConferenceTableEntry 4 }

cmaConferenceIsScheduled OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the conference is scheduled (true) or ad hoc (false)."
::= { cmaActiveConferenceTableEntry 5 }

cmaConferenceIsRecurring OBJECT-TYPE
SYNTAX TruthValue
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Flag indicating whether the conference is a recurring conference."
::= { cmaActiveConferenceTableEntry 6 }

cmaConferenceStartTime OBJECT-TYPE
SYNTAX DateAndTime
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Time of the conference start."
::= { cmaActiveConferenceTableEntry 7 }
MAX-ACCESS  read-only
STATUS       current
DESCRIPTION  “Start date/time of the conference.”
::= { cmaActiveConferenceTableEntry 7 }

cmaConferenceOwner OBJECT-TYPE
SYNTAX        OCTET STRING (SIZE(0..255))
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Owner of the conference.”
::= { cmaActiveConferenceTableEntry 8 }

cmaConferenceStatus OBJECT-TYPE
SYNTAX        CmaConferenceStatus
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Status of the conference.”
::= { cmaActiveConferenceTableEntry 9 }

cmaConferenceTotalParticipants OBJECT-TYPE
SYNTAX        Integer32
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Total number of participants for the conference (both connected
and disconnected).”
::= { cmaActiveConferenceTableEntry 10 }

cmaConferenceConnectedParticipants OBJECT-TYPE
SYNTAX        Integer32
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Number of connected participants for the conference.”
::= { cmaActiveConferenceTableEntry 11 }

cmaConferenceIsCascaded OBJECT-TYPE
SYNTAX        TruthValue
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Flag indicating whether the conference is cascaded.”
::= { cmaActiveConferenceTableEntry 12 }

cmaConferenceMcu OBJECT-TYPE
SYNTAX        OCTET STRING (SIZE(0..255))
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Name of the MCU hosting the conference. Empty if no MCU is involved.
For cascaded conferences, this is a comma-delimited list of MCUs.”
::= { cmaActiveConferenceTableEntry 13 }

cmaConferenceAvgParticipantAudioQOE OBJECT-TYPE
SYNTAX        Integer32          -- meaning is yet to be defined
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Average audio QOE (Quality Of Experience)
for all connected participants in the conference.”
::= { cmaActiveConferenceTableEntry 14 }

cmaConferenceAvgParticipantVideoQOE OBJECT-TYPE
SYNTAX        Integer32          -- meaning is yet to be defined
MAX-ACCESS    read-only
STATUS current
DESCRIPTION "Average video QOE (Quality Of Experience) for all connected participants in the conference."
 ::= { cmaActiveConferenceTableEntry 15 }

cmaConferenceAvgParticipantContentQOE OBJECT-TYPE
SYNTAX Integer32 -- meaning is yet to be defined
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Average content QOE (Quality Of Experience) for all connected participants in the conference."
 ::= { cmaActiveConferenceTableEntry 16 }

cmaConferenceMinParticipantAudioQOE OBJECT-TYPE
SYNTAX Integer32 -- meaning is yet to be defined
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Minimum audio QOE (Quality Of Experience) across all connected participants in the conference."
 ::= { cmaActiveConferenceTableEntry 17 }

cmaConferenceMinParticipantVideoQOE OBJECT-TYPE
SYNTAX Integer32 -- meaning is yet to be defined
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Minimum video QOE (Quality Of Experience) across all connected participants in the conference."
 ::= { cmaActiveConferenceTableEntry 18 }

cmaConferenceMinParticipantContentQOE OBJECT-TYPE
SYNTAX Integer32 -- meaning is yet to be defined
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Minimum content QOE (Quality Of Experience) across all connected participants in the conference."
 ::= { cmaActiveConferenceTableEntry 19 }

-- END Conference status

-- START system alerts

-- CMA system alerts status conformance group.

-- END System alerts
::= { cmaStatusAlerts 1 }

CmaSystemAlertTableEntry ::= SEQUENCE
{
cmaSystemAlertIndex          CmaDefaultTableIndexRange,
cmaSystemAlertSequenceNumber Counter32,
cmaSystemAlertType           CmaSystemAlertType,
cmaSystemAlertDescription   OCTET STRING,
cmaSystemAlertGenerationTime DateAndTime,
cmaSystemAlertNotes         OCTET STRING
}

cmaSystemAlertTable OBJECT-TYPE
SYNTAX        SEQUENCE OF CmaSystemAlertTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "System alert table. Contains information for all
active alerts."
::= { cmaStatusAlerts 2 }

cmaSystemAlertTableEntry OBJECT-TYPE
SYNTAX        CmaSystemAlertTableEntry
MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION   "System alert table entry."
INDEX         { cmaSystemAlertIndex }
::= { cmaSystemAlertTable 1 }

cmaSystemAlertIndex OBJECT-TYPE
SYNTAX        CmaDefaultTableIndexRange
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Unique system-assigned ID for this entry."
::= { cmaSystemAlertTableEntry 1 }

cmaSystemAlertSequenceNumber OBJECT-TYPE
SYNTAX        Counter32
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Sequence number of the system alert."
::= { cmaSystemAlertTableEntry 2 }

cmaSystemAlertType OBJECT-TYPE
SYNTAX        CmaSystemAlertType
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Alert type of the system alert."
::= { cmaSystemAlertTableEntry 3 }

cmaSystemAlertDescription OBJECT-TYPE
SYNTAX        OCTET STRING
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   "Description of the system alert."
::= { cmaSystemAlertTableEntry 4 }

cmaSystemAlertGenerationTime OBJECT-TYPE
SYNTAX        DateAndTime
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION "Date and time when the system alert was generated."
::= { cmaSystemAlertTableEntry 5 }  

cmaSystemAlertNotes OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Notes for the system alert."
::= { cmaSystemAlertTableEntry 6 }  

-- END system alerts

-- START Redundancy status

cmaStatusRedundancyGroup OBJECT-GROUP
OBJECTS
{
    cmaRedundancyStatus,
    cmaRedundancyVirtualInetAddressType,
    cmaRedundancyVirtualInetAddress,
    cmaRedundantServerIndex,
    cmaRedundantServerInetAddressType,
    cmaRedundantServerInetAddress,
    cmaRedundantServerRole,
    cmaRedundantServerMachineStatus
}
STATUS current
DESCRIPTION "CMA redundancy status conformance group."
::= { cmaStatusConformance 10 }  

CmaRedundantTableEntry ::= SEQUENCE
{
    cmaRedundantServerIndex CmaDefaultTableIndexRange,
    cmaRedundantServerInetAddressType InetAddressType,
    cmaRedundantServerInetAddress InetAddress,
    cmaRedundantServerRole CmaRedundantServerRole,
    cmaRedundantServerMachineStatus CmaRedundantServerStatus
}
cmaRedundancyTable OBJECT-TYPE
SYNTAX       SEQUENCE OF CmaRedundancyTableEntry
MAX-ACCESS   not-accessible
STATUS       current
DESCRIPTION  "CMA server redundancy table. In a redundant system, it
                includes an entry for each of the two servers."
 ::= {  cmaStatusRedundancy 4 }

CmaRedundancyTableEntry OBJECT-TYPE
SYNTAX       CmaRedundancyTableEntry
MAX-ACCESS   not-accessible
STATUS       current
DESCRIPTION  "CMA server redundancy table entry."
INDEX        {  cmaRedundantServerIndex  }
 ::= {  cmaRedundancyTable 1 }

CmaRedundantServerIndex OBJECT-TYPE
SYNTAX       CmaDefaultTableIndexRange
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Unique system-assigned ID for this entry."
 ::= {  cmaRedundancyTableEntry 1 }

CmaRedundantServerInetAddressType OBJECT-TYPE
SYNTAX       InetAddressType
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "IP address type of the server."
 ::= {  cmaRedundancyTableEntry 2 }

CmaRedundantServerInetAddress OBJECT-TYPE
SYNTAX       InetAddress
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "IP address of the server."
 ::= {  cmaRedundancyTableEntry 3 }

CmaRedundantServerRole OBJECT-TYPE
SYNTAX       CmaRedundantServerRole
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Role of the server."
 ::= {  cmaRedundancyTableEntry 4 }

CmaRedundantServerMachineStatus OBJECT-TYPE
SYNTAX       CmaRedundantServerStatus
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  "Machine status of the server."
 ::= {  cmaRedundancyTableEntry 6 }

-- END Redundancy status

-- START Site statistics

cmaStatusSitesGroup OBJECT-GROUP
OBJECTS
{
turn on ntp

```
cmaSiteCount,  
cmaSiteIndex,  
cmaSiteName,  
cmaSiteCallCount,  
cmaSiteBandwidthUsed,  
cmaSiteBandwidthTotal,  
cmaSiteAverageCallBitRate,  
cmaSitePacketLoss,  
cmaSiteAverageJitter,  
cmaSiteAverageDelay,  
cmaSiteLinkCount,  
cmaSiteLinkIndex,  
cmaSiteLinkName,  
cmaSiteLinkFromSite,  
cmaSiteLinkToSite,  
cmaSiteLinkCallCount,  
cmaSiteLinkBandwidthUsed,  
cmaSiteLinkBandwidthTotal,  
cmaSiteLinkAverageCallBitRate,  
cmaSiteLinkPacketLoss,  
cmaSiteLinkAverageJitter,  
cmaSiteLinkAverageDelay,  
cmaSubnetCount,  
cmaSubnetIndex,  
cmaSubnetName,  
cmaSubnetSiteName,  
cmaSubnetCallCount,  
cmaSubnetBandwidthUsed,  
cmaSubnetBandwidthTotal,  
cmaSubnetAverageCallBitRate,  
cmaSubnetPacketLoss,  
cmaSubnetAverageJitter,  
cmaSubnetAverageDelay
```

```c
}  
STATUS current  
DESCRIPTION "CMA sites status conformance group."  
::= { cmaStatusConformance 11 }
```

cmaSiteCount OBJECT-TYPE  
SYNTAX Integer32  
MAX-ACCESS read-only  
STATUS current  
DESCRIPTION "Number of sites provisioned in the CMA server."  
::= { cmaStatusSites 1 }

cmaSiteTableEntry ::= SEQUENCE  
{
  cmaSiteIndex CmaDefaultTableIndexRange,  
cmaSiteName OCTET STRING,  
cmaSiteCallCount Integer32,  
cmaSiteBandwidthUsed Integer32,  
cmaSiteBandwidthTotal Counter64,  
cmaSiteAverageCallBitRate Counter64,  
cmaSitePacketLoss Integer32,  
cmaSiteAverageJitter Integer32,  
cmaSiteAverageDelay Integer32
}

cmaSiteTable OBJECT-TYPE  
SYNTAX SEQUENCE OF CmaSiteTableEntry
```
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION “CMA site table. Contains usage and network quality information for the sites. Only CMA controlled sites will be included in this table.”
::= { cmaStatusSites 2 }
cmaSiteTableEntry OBJECT-TYPE
SYNTAX  CmaSiteTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION “CMA site table entry.”
INDEX { cmaSiteIndex }
::= { cmaSiteTable 1 }
cmaSiteIndex OBJECT-TYPE
SYNTAX  CmADefaultTableIndexRange
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Unique system-assigned ID for this entry.”
::= { cmaSiteTableEntry 1 }
cmaSiteName OBJECT-TYPE
SYNTAX  OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Name of the site.”
::= { cmaSiteTableEntry 2 }
cmaSiteCallCount OBJECT-TYPE
SYNTAX  Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Number of active calls in the site.”
::= { cmaSiteTableEntry 3 }
cmaSiteBandwidthUsed OBJECT-TYPE
SYNTAX  Integer32 (0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Percentage of bandwidth used in the site.”
::= { cmaSiteTableEntry 4 }
cmaSiteBandwidthTotal OBJECT-TYPE
SYNTAX  Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Total bandwidth used in the site.”
::= { cmaSiteTableEntry 5 }
cmaSiteAverageCallBitRate OBJECT-TYPE
SYNTAX  Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Average call bit rate in the site.”
::= { cmaSiteTableEntry 6 }
cmaSitePacketLoss OBJECT-TYPE
SYNTAX  Integer32 (0..100)
MAX-ACCESS read-only
STATUS          current
DESCRIPTION     “Percentage of packet loss in the site.”
::= { cmaSiteTableEntry 7 }


cmaSiteAverageJitter OBJECT-TYPE
SYNTAX          Integer32
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION     “Average jitter in the site.”
::= { cmaSiteTableEntry 8 }


cmaSiteAverageDelay OBJECT-TYPE
SYNTAX          Integer32
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION     “Average delay in the site.”
::= { cmaSiteTableEntry 9 }

-- END Site statistics

-- START Site link statistics

cmaSiteLinkCount OBJECT-TYPE
SYNTAX          Integer32
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION     “Number of site links provisioned in the CMA server.”
::= { cmaStatusSiteLinks 1 }

CmaSiteLinkTableEntry ::= SEQUENCE
{
cmaSiteLinkIndex CmaDefaultTableIndexRange,
cmaSiteLinkName OCTET STRING,
cmaSiteLinkFromSite OCTET STRING,
cmaSiteLinkToSite OCTET STRING,
cmaSiteLinkCallCount Integer32,
cmaSiteLinkBandwidthUsed Integer32,
cmaSiteLinkBandwidthTotal Counter64,
cmaSiteLinkAverageCallBitRate Counter64,
cmaSiteLinkPacketLoss Integer32,
cmaSiteLinkAverageJitter Integer32,
cmaSiteLinkAverageDelay Integer32
}

CmaSiteLinkTable OBJECT-TYPE
SYNTAX          SEQUENCE OF CmaSiteLinkTableEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     “CMA site link table. Contains usage and network
                quality information for the site links. Only site links
                with at least one CMA controlled site will be included
                in this table”
::= { cmaStatusSiteLinks 2 }

CmaSiteLinkTableEntry OBJECT-TYPE
SYNTAX          CmaSiteLinkTableEntry
MAX-ACCESS      not-accessible
STATUS          current
DESCRIPTION     “CMA site link table entry.”
INDEX  { cmaSiteLinkIndex }
::= { cmaSiteLinkTable 1 }

cmaSiteLinkIndex  OBJECT-TYPE
SYNTAX        CmaDefaultTableIndexRange
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Unique system-assigned ID for this entry.”
::= { cmaSiteLinkTableEntry 1 }

cmaSiteLinkName  OBJECT-TYPE
SYNTAX        OCTET STRING (SIZE(1..255))
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Name of the site link.”
::= { cmaSiteLinkTableEntry 2 }

cmaSiteLinkFromSite  OBJECT-TYPE
SYNTAX        OCTET STRING (SIZE(1..255))
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Name of the site of origin for the link.”
::= { cmaSiteLinkTableEntry 3 }

cmaSiteLinkToSite  OBJECT-TYPE
SYNTAX        OCTET STRING (SIZE(1..255))
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Name of the destination site for the link.”
::= { cmaSiteLinkTableEntry 4 }

cmaSiteLinkCallCount  OBJECT-TYPE
SYNTAX        Integer32
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Number of active calls in the link.”
::= { cmaSiteLinkTableEntry 5 }

cmaSiteLinkBandwidthUsed  OBJECT-TYPE
SYNTAX        Integer32 (0..100)
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Percentage of bandwidth used in the link.”
::= { cmaSiteLinkTableEntry 6 }

cmaSiteLinkBandwidthTotal  OBJECT-TYPE
SYNTAX        Counter64
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Total bandwidth used in the link.”
::= { cmaSiteLinkTableEntry 7 }

cmaSiteLinkAverageCallBitRate  OBJECT-TYPE
SYNTAX        Counter64
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Average call bit rate in the link.”
::= { cmaSiteLinkTableEntry 8 }

cmaSiteLinkPacketLoss  OBJECT-TYPE
SYNTAX Integer32 (0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Percentage of packet loss in the link.”
::= { cmaSiteLinkTableEntry 9 }

cmaSiteLinkAverageJitter OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Average jitter in the link.”
::= { cmaSiteLinkTableEntry 10 }

cmaSiteLinkAverageDelay OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Average delay in the link.”
::= { cmaSiteLinkTableEntry 11 }

-- END Site link statistics

-- START Subnet statistics

cmaSubnetCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION “Number of subnets provisioned in the CMA server.”
::= { cmaStatusSubnets 1 }

CmaSubnetTableEntry ::= SEQUENCE
{ cmaSubnetIndex CmaDefaultTableIndexRange,
cmaSubnetName OCTET STRING,
cmaSubnetSiteName OCTET STRING,
cmaSubnetCallCount Integer32,
cmaSubnetBandwidthUsed Integer32,
cmaSubnetBandwidthTotal Counter64,
cmaSubnetAverageCallBitRate Counter64,
cmaSubnetPacketLoss Integer32,
cmaSubnetAverageJitter Integer32,
cmaSubnetAverageDelay Integer32 }

CmaSubnetTable OBJECT-TYPE
SYNTAX SEQUENCE OF CmaSubnetTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION “CMA subnet table. Contains usage and network quality information for the Subnets. Only subnets that are contained within CMA controlled sites will be included in this table.”
::= { cmaStatusSubnets 2 }

CmaSubnetTableEntry OBJECT-TYPE
SYNTAX CmaSubnetTableEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION “CMA subnet table entry.”
INDEX { cmaSubnetIndex }
::= { cmaSubnetTable 1 }

cmaSubnetIndex OBJECT-TYPE
SYNTAX CmaDefaultTableIndexRange
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Unique system-assigned ID for this entry."
::= { cmaSubnetTableEntry 1 }

cmaSubnetName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the subnet."
::= { cmaSubnetTableEntry 2 }

cmaSubnetSiteName OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(1..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the subnet's site."
::= { cmaSubnetTableEntry 3 }

cmaSubnetCallCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Number of active calls in the subnet."
::= { cmaSubnetTableEntry 4 }

cmaSubnetBandwidthUsed OBJECT-TYPE
SYNTAX Integer32 (0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Percentage of bandwidth used in the Subnet."
::= { cmaSubnetTableEntry 5 }

cmaSubnetBandwidthTotal OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Total bandwidth used in the subnet."
::= { cmaSubnetTableEntry 6 }

cmaSubnetAverageCallBitRate OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Average call bit rate in the subnet."
::= { cmaSubnetTableEntry 7 }

cmaSubnetPacketLoss OBJECT-TYPE
SYNTAX Integer32 (0..100)
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Percentage of packet loss in the subnet."
::= { cmaSubnetTableEntry 8 }

cmaSubnetAverageJitter OBJECT-TYPE
SYNTAX        Integer32
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Average jitter in the subnet.”
 ::= { cmaSubnetTableEntry 9 }

cmaSubnetAverageDelay OBJECT-TYPE
SYNTAX        Integer32
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION   “Average delay in the subnet.”
 ::= { cmaSubnetTableEntry 10 }

-- END Subnet statistics

-- Alert Group

alertGroup OBJECT-GROUP
OBJECTS
{
  alertSequenceNumber,
  alertSeverity,
  alertTimeStamp,
  alertFailedServerInetAddressType,
  alertFailedServerInetAddress,
  alertActiveServerInetAddressType,
  alertActiveServerInetAddress,
  alertRedundantServerInetAddressType,
  alertRedundantServerInetAddress,
  alertCmaServerInetAddressType,
  alertCmaServerInetAddress,
  alertMcuName,
  alertCmaDbName,
  alertSiteName,
  alertSubnetInetAddressType,
  alertSubnetInetAddress,
  alertSubnetMask,
  alertSiteLinkName,
  alertBandwidthInUse,
  alertBandwidthThreshold,
  alertAuditLogSizeUsed,
  alertAuditLogSizeThreshold,
  alertDiskSpaceUsage,
  alertCertificationExpirationWarning,
  alertCertificationExpiredWarning,
  alertCpuUsageExceeded,
  alertMemoryUsageExceeded,
  alertDmaName
}
$STATUS current
DESCRIPTION "A collection of alert-related objects."
 ::= { cmaNotificationConformance 1 }

alertSequenceNumber OBJECT-TYPE
SYNTAX        Counter32
MAX-ACCESS    accessible-for-notify
STATUS        current
DESCRIPTION   "Sequential ID number of the alert. Each alert ID
on a specific CMA server is unique."
::= { cmaAlertObjectsGeneral 1 }

alertSeverity OBJECT-TYPE
SYNTAX   ItuPerceivedSeverity
MAX-ACCESS accessible-for-notify
STATUS   current
DESCRIPTION "Severity of the alert."
::= { cmaAlertObjectsGeneral 2 }

alertTimeStamp OBJECT-TYPE
SYNTAX   DateAndTime
MAX-ACCESS accessible-for-notify
STATUS   current
DESCRIPTION "Timestamp of the alert."
::= { cmaAlertObjectsGeneral 3 }

alertFailedServerInetAddressType OBJECT-TYPE
SYNTAX   InetAddressType
MAX-ACCESS accessible-for-notify
STATUS   current
DESCRIPTION "IP address type of the failed CMA server."
::= { cmaAlertObjectsGeneral 4 }

alertFailedServerInetAddress OBJECT-TYPE
SYNTAX   InetAddress
MAX-ACCESS accessible-for-notify
STATUS   current
DESCRIPTION "IP address of the failed CMA server."
::= { cmaAlertObjectsGeneral 5 }

alertActiveServerInetAddressType OBJECT-TYPE
SYNTAX   InetAddressType
MAX-ACCESS accessible-for-notify
STATUS   current
DESCRIPTION "IP address type of the active CMA server."
::= { cmaAlertObjectsGeneral 6 }

alertActiveServerInetAddress OBJECT-TYPE
SYNTAX   InetAddress
MAX-ACCESS accessible-for-notify
STATUS   current
DESCRIPTION "IP address of the active CMA server."
::= { cmaAlertObjectsGeneral 7 }

alertRedundantServerInetAddressType OBJECT-TYPE
SYNTAX   InetAddressType
MAX-ACCESS accessible-for-notify
STATUS   current
DESCRIPTION "IP address type of the redundant CMA server."
::= { cmaAlertObjectsGeneral 8 }

alertRedundantServerInetAddress OBJECT-TYPE
SYNTAX   InetAddress
MAX-ACCESS accessible-for-notify
STATUS   current
DESCRIPTION "IP address of the redundant CMA server."
::= { cmaAlertObjectsGeneral 9 }

alertCmaServerInetAddressType OBJECT-TYPE
SYNTAX   InetAddressType
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "IP address type of the CMA server."
::= { cmaAlertObjectsGeneral 10 }

alertCmaServerInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "IP address of the CMA server."
::= { cmaAlertObjectsGeneral 11 }

alertMcuName OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name assigned to an MCU within the CMA"
::= { cmaAlertObjectsGeneral 12 }

alertCmaDbName OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA Database name."
::= { cmaAlertObjectsGeneral 15 }

alertSiteName OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the site."
::= { cmaAlertObjectsGeneral 18 }

alertSubnetInetAddressType OBJECT-TYPE
SYNTAX InetAddressType
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address type of the subnet."
::= { cmaAlertObjectsGeneral 19 }

alertSubnetInetAddress OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "IP address of the subnet."
::= { cmaAlertObjectsGeneral 20 }

alertSubnetMask OBJECT-TYPE
SYNTAX InetAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Subnet mask for the subnet."
::= { cmaAlertObjectsGeneral 21 }

alertSiteLinkName OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Name of the site link."
::= { cmaAlertObjectsGeneral 22 }
alertBandwidthInUse OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Bandwidth in use for site, site link, or subnet being reported."
::= { cmaAlertObjectsGeneral 23 }

alertBandwidthThreshold OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Threshold that has been exceeded."
::= { cmaAlertObjectsGeneral 24 }

alertAuditLogSizeUsed OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Disc space used by audit log(s)."
::= { cmaAlertObjectsGeneral 25 }

alertAuditLogSizeThreshold OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Audit log size threshold that has been exceeded."
::= { cmaAlertObjectsGeneral 26 }

alertDiskSpaceUsage OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Disk space usage threshold has been exceeded message."
::= { cmaAlertObjectsGeneral 27 }

alertCertificationExpirationWarning OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA Certification is nearing expiration."
::= { cmaAlertObjectsGeneral 28 }

alertCertificationExpiredWarning OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CMA Certificate has expired."
::= { cmaAlertObjectsGeneral 29 }

alertCPUUsageExceeded OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION "CPU Usage threshold has been exceeded message."
::= { cmaAlertObjectsGeneral 30 }

alertMemoryUsageExceeded OBJECT-TYPE
SYNTAX OCTET STRING(SIZE (0..255))
MAX-ACCESS read-only
STATUS       current
DESCRIPTION  “Memory Usage threshold has been exceeded message.”
::= { cmaAlertObjectsGeneral 31 }

alertDmaName OBJECT-TYPE
SYNTAX       OCTET STRING(SIZE (0..255))
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION  “Name assigned to a DMA within the CMA”
::= { cmaAlertObjectsGeneral 32 }

-------------------------------------------------------------------------------
-- Alerts
-------------------------------------------------------------------------------
cmaAlertNotificationGroup  NOTIFICATION-GROUP
NOTIFICATIONS
{ mcuDownAlert,
  dbConnectionDownAlert,
  ldapConnectionDownAlert,
  cmaFailoverAlert,
  licenseCapacityAlert,
  mcuTimeDiscrepancyAlert,
  cmaMonitorServiceStoppedAlert,
  redundantServerDownAlert,
  redundantServerConflictAlert,
  ldapSystemAccountPasswordFailed,
  ldapConnectionFailed,
  bandwidthUsedSiteAlert,
  bandwidthUsedSubnetAlert,
  bandwidthUsedSiteLinkAlert,
  auditUsageThresholdExceeded,
  alertDiskSpaceUsageExceeded,
  certificationExpirationWarning,
  certificationExpiredWarning,
  cpuUsageExceeded,
  memoryUsageExceeded,
  dmaDownAlert
}
STATUS       current
DESCRIPTION  “Notifications that the CMA SNMP agent is required to implement.”
::= { cmaNotificationConformance 2 }

mcuDownAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertMcuName }
STATUS       current
DESCRIPTION  “Alert generated when the CMA server detects a loss of communication with an MCU.”
::= { cmaAlertObjectsAlerts 1 }

dbConnectionDownAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertCmaDbName }
STATUS       current
DESCRIPTION  “Alert generated when the CMA server detects a connection loss with the CMA database.”
::= { cmaAlertObjectsAlerts 2 }

ldapConnectionDownAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp }
STATUS       current
DESCRIPTION
"Alert generated when the CMA server detects a connection loss with the LDAP server."
::= { cmaAlertObjectsAlerts 3 }

cmaFailoverAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp,
          alertFailedServerInetAddressType, alertFailedServerInetAddress,
          alertActiveServerInetAddressType, alertActiveServerInetAddress }
STATUS       current
DESCRIPTION
"Alert generated when the CMA server fails over to the redundant server."
::= { cmaAlertObjectsAlerts 4 }

licenseCapacityAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp }
STATUS       current
DESCRIPTION
"Alert generated when the percentage of used licenses reaches 5% of the maximum."
::= { cmaAlertObjectsAlerts 5 }

mcuTimeDiscrepancyAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertMcuName }
STATUS       current
DESCRIPTION
"Alert generated when the CMA server detects a discrepancy between the CMA system
time and the time reported on an MCU."
::= { cmaAlertObjectsAlerts 6 }

cmaMonitorServiceStoppedAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertCmaServerInetAddressType,
          alertCmaServerInetAddress }
STATUS       current
DESCRIPTION
"Alert generated when the CMA redundancy monitoring service stops on a CMA server.
Contains the IP address of the server on which the monitoring service has stopped."
::= { cmaAlertObjectsAlerts 7 }

redundantServerDownAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertFailedServerInetAddressType,
          alertFailedServerInetAddress }
STATUS       current
DESCRIPTION
"Alert generated when the CMA server detects a connection loss with the
redundant CMA server."
::= { cmaAlertObjectsAlerts 8 }

redundantServerConflictAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertActiveServerInetAddressType,
          alertActiveServerInetAddress, alertRedundantServerInetAddressType, alertRedundantServerInetAddress }
STATUS       current
DESCRIPTION
"Alert generated if the active and redundant CMA servers are both
running in active mode."
::= { cmaAlertObjectsAlerts 9 }

ldapSystemAccountPasswordFailed NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp }
STATUS       current
DESCRIPTION
“Alert generated if the CMA server cannot connect to the LDAP server using
the configured LDAP system account.”
::= { cmaAlertObjectsAlerts 10 }

ldapConnectionFailed NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp }
STATUS       current
DESCRIPTION
“Alert generated if the connection to the previously connected LDAP server fails.”
::= { cmaAlertObjectsAlerts 11 }

bandwidthUsedSiteAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertSiteName,
          alertBandwidthInUse, alertBandwidthThreshold }
STATUS       current
DESCRIPTION
“Alert generated when the CMA server detects bandwidth usage for a site
has exceeded an upper threshold.”
::= { cmaAlertObjectsAlerts 12 }

bandwidthUsedSubnetAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertSiteName,
           alertSubnetInetAddressType, alertSubnetInetAddress, alertSubnetMask,
           alertBandwidthInUse, alertBandwidthThreshold }
STATUS       current
DESCRIPTION
“Alert generated when the CMA server detects bandwidth usage for a site has exceeded an upper
threshold.”
::= { cmaAlertObjectsAlerts 13 }

bandwidthUsedSiteLinkAlert NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertSiteLinkName,
          alertBandwidthInUse, alertBandwidthThreshold }
STATUS       current
DESCRIPTION
“Alert generated when the CMA server detects bandwidth usage for a site has exceeded an upper
threshold.”
::= { cmaAlertObjectsAlerts 14 }

auditUsageThresholdExceeded NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertAuditLogSizeUsed,
           alertAuditLogSizeThreshold }
STATUS       current
DESCRIPTION
“Alert generated when the disc usage for audit logs exceeds the defined threshold.”
::= { cmaAlertObjectsAlerts 15 }

alertDiskSpaceUsageExceeded NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertDiskSpaceUsage }
STATUS       current
DESCRIPTION
“Alert generated when the disc usage for the system exceeds the defined threshold.”
::= { cmaAlertObjectsAlerts 16 }

certificationExpirationWarning NOTIFICATION-TYPE
OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertCertificationExpirationWarning }
STATUS       current
DESCRIPTION
“Alert generated when the CMA certificate is nearing expiration.”
::= { cmaAlertObjectsAlerts 17 }
certificationExpiredWarning NOTIFICATION-TYPE
   OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertCertificationExpiredWarning }
   STATUS       current
   DESCRIPTION  “Alert generated when the CMA certificate is expired.”
::= { cmaAlertObjectsAlerts 18 }
cpuUsageExceeded NOTIFICATION-TYPE
   OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertCpuUsageExceeded }
   STATUS       current
   DESCRIPTION  “Alert generated when the CPU Usage is exceeding the defined threshold.”
::= { cmaAlertObjectsAlerts 19 }
memoryUsageExceeded NOTIFICATION-TYPE
   OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertMemoryUsageExceeded }
   STATUS       current
   DESCRIPTION  “Alert generated when the memory usage is exceeding the defined threshold.”
::= { cmaAlertObjectsAlerts 20 }
dmaDownAlert NOTIFICATION-TYPE
   OBJECTS { alertSequenceNumber, alertSeverity, alertTimeStamp, alertDmaName }
   STATUS       current
   DESCRIPTION  “Alert generated when the CMA server detects a loss of communication with a DMA.”
::= { cmaAlertObjectsAlerts 21 }
END
Index

MCU and gateway dialing problems 522

A
Acknowledge Help command 56, 61
activation keys, requesting 105
active conference. See conference
Add Device command 82, 226
adding
conference templates 350
conferences 33
custom logos to the user interface 424, 425
provisioning profiles 134, 146
rooms 356
site links 493
sites 479
system licenses 423
user roles 293
users to the system 279
adding manually
endpoints 90
MCUs 233
admin/monitor view commands
Clear Help 83
Delete Device 82, 226
Edit Device 82, 226
Manage Device 83
Manage User 83
Reboot Device 83
Send Message 83
View Device Details 82
administering a redundant system 441
Adobe Flash Player 3
advanced conference settings
editing 47
applications
displaying on peripherals 100
areas
associating users with 295
viewing list of 409
assigning
a lecturer 50
a video chairperson 50
user roles and devices 292
Associate Area command 83
Associate User command 83
associating
  users with areas 295
audio-only conference 34
automatic software updates
  uploading the image 106
available commands, list of 23, 80

B
bandwidth. See bit rate
best practices 511
bit rate
  setting for internal participants 49
bridge (MCU)
  features field names 70
  forcing use of 49

C
call routing
  setting up 11
Cancel Provision command 151
Cancel Update command 125
canceling
  conferences 64
  provisioning 149
  software updates 125
capabilities, system, list of 1
certificate
  remove 455
chairperson
  assigning 50
  enabling 48
  passcode for 48
changing
  advanced conference settings 47
  conference information 41
  conference templates 350
  endpoints 95
  participant dial options 43
  participant endpoint settings 43
  permissions for a user role 294
  provisioning profiles 135, 136, 146
  rooms 359
  site links 493
  site settings 490
  system network settings 415
  system time settings 416
  user information 281
checking the status of endpoint provisioning 148
Clear Help command 83
Clear Status command 125, 151
clearing
  endpoint help requests 97
  status of endpoint provisioning 149
cloning provisioning profiles 136, 147
closing the Resource Manager system 7
command categories
  admin/monitor view commands 82, 226
  admin/peripheral view commands 85
  software update view commands 124
commands
  Acknowledge Help 56, 61
  Add Device 82, 226
  Associate Area 83
  Associate User 83
  Cancel Provision 151
  Cancel Update 125
  Clear Help 83
  Clear Status 125, 151
  Connect/Disconnect participant 55, 60
  Delete Conference 26
  Delete Device 82, 226
  Delete Peripheral 85
  Display Applications 85
  Edit Conference 26, 27
  Edit Device 82, 226
  list of 23, 80
  Manage Conference 27
  Manage Device 83
  Manage User 83
  Provision 151
  Reboot Device 83
  Remove Participant 55, 61
  Search Devices 82
  Send Message 55, 61, 83
  Software Update 125
  Terminate Conference 27
  View Device Details 82
  View Peripherals 83
commands, dashboard
  Refresh 322
  Restart 322
  Shutdown 322
conference details
  conference details field names 65
displaying 23
conference features field names 68
conference rooms
  adding 40
conference settings
  editing 47
conference settings. See settings
conference templates
adding 350
deleting 351
editing 350
overview of 334
setting up 12
viewing list of 349

custom
    custom logo, adding to the user interface 424, 425

Custom Date filter 24
customizing the user interface 424, 425

D

dashboard 321
dashboard commands
    Refresh 322
    Restart 322
    Shutdown 322
data plus video stream 50
database
    overview 437
databases
    restoring, overview of 437
Delete Conference command 26
Delete Device command 82, 226
Delete Peripheral command 85

Connect/Disconnect Participant command 55, 60
connection speed
    setting for internal participants 49
continuous presence mode 49, 55
copying
    provisioning profiles 136, 147
creating
    conferences 33
custom
    custom logo, adding to the user interface 424, 425

Delete Conference command 26
Delete Device command 82, 226
Delete Peripheral command 85

configuring
    a redundant system 439
    an LDAP connection 10
    endpoints 127, 131, 139, 143
    redundancy 11
    software updates for peripherals for production 118
    software updates for peripherals for trial 120

configuration speed
    setting for internal participants 49
continuing presence mode 49, 55
copying
    provisioning profiles 136, 147
creating
    conferences 33

dashboard 321
dashboard commands
    Refresh 322
    Restart 322
    Shutdown 322
data plus video stream 50
database
    overview 437
databases
    restoring, overview of 437
Delete Conference command 26
Delete Device command 82, 226
Delete Peripheral command 85
deleting
conference templates 351
conferences 64
endpoints 95
peripherals 100
provisioning profiles 137, 147
rooms 359
site links 494
sites 491
user roles 294
users 283
deleting a conference 26
details of conference, displaying 23
device commands
Add Device 82, 226
Associate Area 83
Associate User 83
Delete Peripheral 85
Display Applications 85
Search Devices 82
View Peripherals 83
device details
alias 87, 93, 216, 247
audio protocol 218
available to schedule 88, 94, 214, 232, 237, 246
call type 218
capabilities enabled 88, 94, 215, 232, 237, 247
cause code 218
description 86, 230, 235
device local time 217
Directory registration 216
encryption 218
endpoint ISDN type 217
errors 219
far site name 218
far site number 218
gatekeeper registration 216
HTTP port 87, 92, 231, 236
HTTP URL 87, 92, 231, 236
IP address 82, 86, 103, 213, 230, 235, 246
ISDN assignment type 217
ISDN line status type 217
ISDN video number 87, 93, 214, 231, 236, 246
monitoring level 88, 94, 214
name 86
owner 213
serial number 86, 214, 230, 235, 246
site 86, 214, 230, 235, 246
software version 86, 92, 214, 230, 235, 246
supported protocols 88, 94, 215, 231, 236, 247
type 86, 230, 235
video format 218
video protocol 218
warnings 219
device details, viewing 86
device list field names 80
device lists
  list of provisioning details 145
  list of serial numbers for 103
device summary
  name 82, 213, 246
  type 213, 246
devices
  assigning to users 292
device details field names 213, 246
  scheduling software updates for 122
  setting passwords for 75
endpoints
  See also endpoints
devices, managing for participants 60
dial options
  editing 43
  setting 49
dial-in option 49
dial-out option 49
Directory Overview screen 3
directory services
  setting up 13
disconnecting/connecting a participant 55, 60
Display Applications command 85
displaying
  applications on peripherals 100
  areas list 409
  conference templates list 349
  device details 86
  global address book 381
  peripherals 99
  rooms list 356
  system log files 316
  user roles list 292
downloading software updates 104

E
Edit Conference command 26, 27
Edit Device command 82, 226
editing
  advanced conference settings 47
  conference information 41
  conference templates 350
  endpoints 95
  participant dial options 43
  participant endpoint settings 43
  permissions for a user role 294
  provisioning profiles 135, 136, 146
  rooms 359
site links 493
site settings 490
system network settings 415
system time settings 416
user information 281
email notifications 41, 42
enabling a chairperson 48
endpoints
   adding manually 90
canceling provisioning for 149
checking provisioning status for 148
clearing a help request for 97
clearing provisioning status for 149
configuring 127, 131, 139, 143
deleting 95
editing information about 95
editing settings for 43
provisioning 148
provisioning details field names 219
sending messages to 55, 61
setting passwords for 75
software update details field names 220
video feed for 96
entering the system license file 423
exporting
   system log files 316

F
failover, initiating in a redundant system 444
features
   list of conference 23
features, system, list of 1
feed, viewing for a video endpoint 96
field names
   bridge (MCU) features 70
   conference details 65
   conference features 68
device details 213, 246
device list 80
participant details 71
participants 70
peripherals list 84
provisioning details 219
software update details 220
fields
   input requirements for 4
filtering
   overview of 4
filters
   Custom Date 24
   Future Only 24
   Ongoing Plus 24
Today Only 24
Today Plus 24
Yesterday Plus 24
forcing MCU usage 49
future conference view 23
Future Only filter 24

G
gateway dialing, troubleshooting 522
global address book
  viewing 381
guest participants
  adding 37

H
help request, clearing for an endpoint 97
help, acknowledging 56, 61

I
implementing
  a redundant system 442
initiating failover in a redundant system 444
input requirements for fields
  requirements
    for field inputs
      ASCII-only fields 4

K
keys for software activation, requesting 105

L
LDAP 292
LDAP connection, configuring 10
lecturer, assigning 50
license file, requesting 423
licenses, system
  adding 423
    entering number for 423
licensing the system 443
link statistics for a site
  overview of 305
links for a site
  adding 493
    deleting 494
    editing 493
    viewing list of 493
lists
  filtering, overview of 4
    of areas 409
of commands 23, 80
of conference features 23
of conference templates 349
of conferences 23
of device serial numbers 103
of devices 80
of participant details 23
of participants 23
of peripherals 84
of provisioning details 145
of rooms 356
of site links 493
of sites 478
of software updates for peripherals 117
of system features and capabilities 1
of user roles 292
of users 278

logging into the Resource Manager system 3
logging out of the Resource Manager system 7
logo, adding to the user interface 424, 425
logs
  - system log files 316

M
maintenance
  - overview 511
  - recommended 513
Manage Conference command 27
Manage Device command 83
Manage User command 83
management
  - overview 511
  - system 511
managing
  - active conferences 53
  - participant devices 60
manual additions
  - endpoints 90
  - MCUs 233
MCU
  - features field names 70
  - forcing use of 49
MCU details
  - DNS name 230, 235
  - system name 230, 235
MCU device details
  - channels 243
  - international prefix 244
  - LCR table 243
  - local area codes 244
  - local prefix 243
  - non-local prefix 243
number range 243
priority 244
service name 243
MCU dialing, troubleshooting 522
MCUs
  adding manually 233
menus
  System Management 330
messages, sending 55, 61
modes, video
  continuous presence mode 49, 55
  setting 49
  switching mode 49, 55
modifying
  advanced conference settings 47
  conference information 41
  conference templates 350
  endpoints 95
  participant dial options 43
  participant endpoint settings 43
  permissions for a user role 294
  provisioning profiles 135, 136, 146
  rooms 359
  site links 493
  site settings 490
  system network settings 415
  system time settings 416
  user information 281
Monitor Conferences screen 3

N
network settings, editing 415
number for system license, entering 423

O
Ongoing Plus filter 24
open ports
  list of 523
operations
  system 511
overview
  management and maintenance 511

P
participant field names
  participant details field names 71
participants
  adding guest 37
  connecting/disconnecting 55, 60
  list of 23
  list of, details 23
managing devices for 60
removing 55, 61
setting endpoints for 43

participants field names 70

passcodes
  for chairperson 48
  for conferences 48

passwords
  for chairperson 48
  for conference 48

People + Content 50

peripherals
  configuring software updates for production 118
  configuring software updates for trial 120
  deleting 100
  displaying applications on 100
  viewing 99
  viewing list of software updates for 117

peripherals list field names 84

point-to-point calls
  troubleshooting 522

ports used by the Polycom RealPresence Resource Manager system
  list of 524

prereqs_redundancy 441

production
  configuring software updates for peripherals 118

Provision command 151

provision view commands
  Cancel Provision 151
  Clear Status 151
  Provision 151

provisioning
  canceling 149
  provisioning details field names 219
  starting 148

provisioning details
  failure reason 220
  last attempt date/time 220
  last profile applied 219
  log message 220
  pending profile 219
  provisioning status 219
  scheduled 219

provisioning profiles
  adding 134, 146
  cloning 136, 147
  deleting 137, 147
  editing 135, 136, 146
  viewing list of 145
R

Reboot Device command 83
recurring conferences 34
redundancy, configuring 11
redundant system
  administering 441
  configuring 439
  implementing 442
  initiating failover in 444
Refresh command 322
registration
  troubleshooting problems with 521
regular maintenance tasks 513
Remove Participant command 55, 61
removing
  conference templates 351
  conferences 64
  endpoints 95
  peripherals 100
  provisioning profiles 137, 147
  rooms 359
  site links 494
  sites 491
  user roles 294
  users 283
removing a conference 26
request for help, clearing for an endpoint 97
requesting
  software license file 423
requesting update activation keys 105
requirements, system 3
requirements, system, list of 3
Restart command 322
restarting
  the system 7
restoring
  databases, overview of 437
roles, user
  adding 293
  deleting 294
  editing permissions for 294
  overview of 263, 291
  viewing list of 292
rooms
  adding 40, 356
  deleting 359
  editing 359
  viewing list of 356
S

schedule conference view 23
scheduled software updates
  uploading for software updates 106
scheduling a conference 33
scheduling software updates 122
Search Devices command 82
searching
  users 278
Send Message command 55, 61, 83
serial numbers for devices to be updated 103
servers
  initiating failover in a redundant system 444
  updating software for 447
setting up
  conference templates 12
  directory services 13
  video call routing 11
settings
  advanced conference settings 47
  chairperson passcode 48
  conference password 48
  conference settings 347
  connection speed 49
  dial options 49
  enable chairperson 48
  forced MCU usage 49
  network settings 415
  People + Content 50
  system time settings 416
  video mode 49
Shutdown command 322
shutting down the system 7
signed certificate
  remove 455
site link statistics
  overview of 305
site links
  adding 493
  deleting 494
  editing 493
  overview of 491
  viewing list of 493
site settings, editing 490
site statistics
  overview of 303
site topology
  overview of 467
sites
  adding 479
  deleting 491
view graphical topology 478
viewing list of 478
software
requesting license file for 423
updating for the server 447
software update
overview of 101
software update details field names 220
Software Update command 125
software update details
failure reason 111, 221
last attempt date/time 111, 221
log message 111, 221
scheduled 111, 221
software update status 111, 220
software update view commands
Cancel Update 125
Clear Status 125
Software Update 125
software updates
canceling 125
downloading 104
overview of 101
scheduling 122
software updates for peripherals
configuring for production 118
configuring for trial 120
viewing list of 117
starting
the system 7
starting the Resource Manager system 3
statistics
site link statistics, overview of 305
site statistics, overview of 303
status of endpoint provisioning
clearing 149
status of endpoints provisioning
checking 148
stopping
provisioning 149
software updates 125
switching mode 49, 55
system
maintaining 513
operations 511
system dashboard 321
system features and capabilities, list of 1
system licenses
adding 423
entering number for 423
system log files
viewing and exporting 316
system login 3
system management menu 330
system network settings, editing 415
system requirements 3
system requirements, list of 3
system time settings, editing 416
system, licensing 443

T
templates, conference
  adding 350
  deleting 351
  editing 350
  overview of 334
  setting up 12
  viewing list of 349
Terminate Conference command 27
time settings, editing 416
Today Only filter 24
Today Plus filter 24
topology
  of sites 478
  overview of 467
trial
  configuring software updates for peripherals 120
troubleshooting 522
  point-to-point call problems 522
  registration problems 521
Trusted Root CA
  remove 455

U
updates, software
  canceling 125
  downloading 104
  overview of 101
  requesting activation keys for 105
  scheduling 122
updating server software 447
uploading the software image 106
user
  search for a 278
user interface, adding a custom logo to 424, 425
user roles
  adding 293
  deleting 294
  editing permissions for 294
  overview of 263
users
adding to the system 279
assigning roles and devices to 292
associating with areas 295
deleting 283
editing information about 281
overview of 263
roles for 291
searching list of 278

V
video call routing
setting up 11
video chairperson, assigning 50
video endpoints. See devices and endpoints
video feed, viewing for an endpoint 96
video modes
  continuous presence mode 49, 55
  setting 49
  switching mode 49, 55
video plus data stream 50
view
  graphical site topology 478
View Device Details command 82
View Peripherals command 83
viewing
  applications on peripherals 100
  areas list 409
  conference templates list 349
  device details 86
  device serial numbers list 103
  global address book 381
  peripherals 99
  provisioning list and details 145
  rooms list 356
  site links list 493
  sites list 478
  status of endpoint provisioning 148
  system log files 316
  user roles list 292
  video feed for an endpoint 96
views
  future conference view 23
  schedule conference view 23

W
warnings 219
workspaces in the Resource Manager system 3

Y
Yesterday Plus filter 24