Copyright© 2018, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

**Trademarks** Polycom®, the Polycom logo and the names and marks associated with Polycom 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.

![Polycom Logo](image-url)

All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

**Disclaimer** While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

**Limitation of Liability** Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

**End User License Agreement** By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

**Patent Information** The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

**Open Source Software Used in this Product** This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

**Customer Feedback** We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

**Polycom Support** Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.
Contents

Redundancy Status ......................................................... 41
Video Endpoint Licenses (Non-Clariti Only) .......................... 41
Audio and/or Content Endpoint Licenses (Non-Clariti Only) ....... 41
CUCM ........................................................................ 41
DMA .......................................................................... 41
View Alerts .................................................................... 41
Field Input Requirements .................................................. 42
Searching in a List ............................................................ 42
Download Software Packages ............................................. 42
Change a Password ......................................................... 43
Log Out of the System ...................................................... 43
Restart or Shut Down a System .......................................... 43
Shut Down the System in Emergency .................................. 44

Network Configuration ...................................................... 45
Configuring your DNS Server ............................................. 45
Adding DNS SRV Record for RealPresence Resource Manager System Services ........................................... 45
Edit Network Settings ..................................................... 46
Service Interface Settings ................................................ 46
Virtualization Settings ...................................................... 47
Edit Virtualization Settings ............................................... 47
Time Settings .................................................................. 48
Edit System Time Settings ................................................. 48
System Time Settings ...................................................... 48
User Data Collection ....................................................... 48
Enable or Disable User Data Collection ............................... 49
View the Collected Usage Data .......................................... 49

Integrating with an Enterprise Directory .............................. 51
Enterprise Directory Supported Configurations ...................... 51
Single Forest Support ....................................................... 51
Multiple Domains within a Single Forest .............................. 51
Universal Group Support .................................................. 52
Read-only Enterprise Directory Users ................................. 52
How Global Catalog Searches Work ................................... 52
Preparing to Use Active Directory ..................................... 53
LDAP Searches .............................................................. 54
Using the Base DN to Manage Enterprise Directory Searches ........................................................................ 55
Examples of Base DN Filter Expressions .............................. 55
Examples of Base DN Exclusion Filters ............................... 57
Examples of Advanced Base DN Exclusion Filters ................................. 57
RealPresence Resource Manager System and Windows Authentication ............. 58
Managing Directories .................................................................................. 58
   Integrating with Enterprise Directory Server .......................................... 58
      Create the RealPresence Resource Manager System Service Account ....... 59
      Create the RealPresence Resource Manager System Computer Account .... 60
   Enable Integration with the Enterprise Directory Server ......................... 60
Allow Delegated Authentication to Enterprise Directory Server ................. 62
Give Enterprise Users Default Scheduler Role ............................................ 62
Change the Message for Enterprise Users without a Role ......................... 63
Select SMB Version ................................................................................... 63
Endpoint Directory and Directory Settings .................................................. 63
   Global Address Book Tips ....................................................................... 63
   Including or Excluding Dynamically Managed Endpoints in the Global Address Book . 64
      Include Enterprise Users ...................................................................... 64
      Remove Enterprise Users ..................................................................... 64
   Including or Excluding Guest Book Entries in the Directory ..................... 65
      Include Guest Book .............................................................................. 65
      Remove Guest Book ............................................................................ 65
   Allow Local Users to View Enterprise Directory Entries ......................... 65
Supporting LifeSize Endpoints in Directories ............................................... 65
   Modify Directory Listings ......................................................................... 66
   Configure LDAP Settings ......................................................................... 66
   Allow Mid-String Searches for Local Users .............................................. 67
License Management ..................................................................................... 68
License Management ..................................................................................... 69
   System Licensing ..................................................................................... 69
      Video Endpoint and Phones License Control (Non - Polycom RealPresence Clarity) . 70
      Trial Licenses for Appliance Editions ....................................................... 71
      Adding System Licenses for an Appliance Edition for Non - Polycom RealPresence Clarity . 71
         Request a Software License File .......................................................... 71
         Update the License File ...................................................................... 72
   View Current Licensing ............................................................................. 72
   Reclaim Software Client Licenses ............................................................. 73
   Licensing RealPresence Platform Components ........................................... 73
      Managing License for RealPresence Web Suite ..................................... 74
      Managing License for Polycom® ContentConnect™ Solution Server ........ 74
Managing License for a RealPresence DMA Supercluster ................................. 74
Enable Licensing for a Network Device .................................................. 74
Online and Offline Mode ............................................................................ 75
Allocate Licenses for Polycom RealPresence Platform Components ................ 75
Reset Allocated Licenses ............................................................................ 76
Clean Unused Licenses ................................................................................. 76
Update the Licenses of Polycom RealPresence Platform Components .......... 77

System Setup Overview ............................................................................... 79
Setting Up Network Device Management .................................................. 79
Configuring Conferencing ......................................................................... 79
  Setting up Site Topology ........................................................................... 79
  Setting up Conference Templates ............................................................ 80
  Set Up Directory Services ....................................................................... 80
Configuring the Connection to an External Enterprise Directory ................. 80
Setting Up Endpoint Management .............................................................. 81
  Scheduled Management of Endpoints (Polycom and Third-Party) .............. 81
  Dynamic Management of Endpoints (Polycom Only) ................................ 81
Setting up Phones Management ................................................................ 82
Securing the System .................................................................................... 82
Configuring Redundancy (Optional) ............................................................ 82
Distributing Polycom Applications .............................................................. 82

Network Device Management ................................................................. 83

Understanding Network Device Management ......................................... 84
  Overview of Network Device Management .............................................. 84
  Service Integration ................................................................................... 84
  Monitoring ............................................................................................... 84
  Service Group Administration ................................................................. 84
  Licensing ................................................................................................. 85
Supported Network Devices ...................................................................... 85
Network Device Types ............................................................................... 85

Managing Instances .................................................................................. 87
  View Network Device Instance ............................................................... 87
  Network Device Details .......................................................................... 87
  Add an Instance by IP ............................................................................. 88
  Edit an Instance ....................................................................................... 89
  View an Instance ..................................................................................... 89
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete an Instance</td>
<td>89</td>
</tr>
<tr>
<td>Managing Service Groups</td>
<td>90</td>
</tr>
<tr>
<td>Create a Service Group</td>
<td>90</td>
</tr>
<tr>
<td>Edit Service Group Details</td>
<td>91</td>
</tr>
<tr>
<td>Delete a Service Group</td>
<td>91</td>
</tr>
<tr>
<td>Configuring Common Settings for a Service Group</td>
<td>91</td>
</tr>
<tr>
<td>Configure Time Settings for a Service Group</td>
<td>91</td>
</tr>
<tr>
<td>Configure SNMP Settings for a Service Group</td>
<td>92</td>
</tr>
<tr>
<td>Agent Settings</td>
<td>93</td>
</tr>
<tr>
<td>Notification Settings</td>
<td>94</td>
</tr>
<tr>
<td>Adding Security User Settings</td>
<td>94</td>
</tr>
<tr>
<td>Integrate a Service Group with Enterprise Directory</td>
<td>95</td>
</tr>
<tr>
<td>Enterprise Directory Integration Settings</td>
<td>96</td>
</tr>
<tr>
<td>Manage a Network Device within a Service Group</td>
<td>97</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>98</td>
</tr>
<tr>
<td>Service Integration with a RealPresence DMA System</td>
<td>99</td>
</tr>
<tr>
<td>Integration Overview</td>
<td>99</td>
</tr>
<tr>
<td>Dedicated User Account for Integration</td>
<td>99</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>100</td>
</tr>
<tr>
<td>MCU Management</td>
<td>100</td>
</tr>
<tr>
<td>Conference Types Supported By the RealPresence DMA system</td>
<td>100</td>
</tr>
<tr>
<td>RealPresence DMA Conference Templates</td>
<td>100</td>
</tr>
<tr>
<td>Multi-Tenancy Considerations</td>
<td>101</td>
</tr>
<tr>
<td>Considerations for Site Topology</td>
<td>101</td>
</tr>
<tr>
<td>Scheduling Capacity</td>
<td>101</td>
</tr>
<tr>
<td>Integrating with a RealPresence DMA Supercluster</td>
<td>101</td>
</tr>
<tr>
<td>Integrating with a RealPresence DMA system</td>
<td>102</td>
</tr>
<tr>
<td>Requirements of Dedicated RealPresence DMA User Account</td>
<td>102</td>
</tr>
<tr>
<td>Add a RealPresence DMA system by IP Address</td>
<td>102</td>
</tr>
<tr>
<td>Polycrm RealPresence DMA Integration Settings</td>
<td>103</td>
</tr>
<tr>
<td>Configure the Default Territory</td>
<td>104</td>
</tr>
<tr>
<td>Managing a RealPresence DMA System</td>
<td>104</td>
</tr>
<tr>
<td>Edit a RealPresence DMA system</td>
<td>104</td>
</tr>
<tr>
<td>Stop the Service Integration for a RealPresence DMA system</td>
<td>105</td>
</tr>
<tr>
<td>Working with RealPresence DMA Pool Orders</td>
<td>105</td>
</tr>
<tr>
<td>View Details of a RealPresence DMA system Pool Order</td>
<td>106</td>
</tr>
<tr>
<td>DMA Pool Order Details</td>
<td>106</td>
</tr>
</tbody>
</table>
Associate a RealPresence DMA system Pool Order with an Area .......................... 106
Working with Endpoints Synchronized from a RealPresence DMA System .............. 107
Unique H.323 Aliases Required ................................................................. 108
Monitor RealPresence DMA-Synchronized Endpoints ........................................... 108
Schedule RealPresence DMA-Synchronized Endpoints in Conferences ..................... 108
Licensing Threshold for RealPresence DMA-Synchronized H.323 Endpoints .......... 109
  Threshold for Stopping Synchronization .................................................. 109
  Threshold for Deleting Inactive Synchronized H.323 Endpoints ...................... 109

Service Integration with Session Border Controllers ........................................... 110
  Supported Session Border Controllers ...................................................... 110
  Managing Polycom VBP Devices ............................................................... 110
    Add a Polycom VBP Device ................................................................. 110
      Adding Polycom VBP Settings ............................................................ 111
    Edit a Polycom VBP Device ............................................................... 111
    Delete a Polycom VBP Device ............................................................. 111
    Identify Endpoints Using the Polycom VBP Device ................................... 111
  Managing a Polycom RealPresence Access Director System ............................... 112
    Manually Add a RealPresence Access Director System ................................ 112
      Adding a RealPresence Access Director System Settings ........................... 113
    Managing SBC Devices ........................................................................... 113
      Add an SBC Device .............................................................................. 113
        Adding an SBC Device Settings .......................................................... 114
      Edit an SBC Device ............................................................................. 114
      Delete an SBC Device ......................................................................... 114
      Identify Endpoints Using the SBC Device .............................................. 114

Service Integration with Bridges ................................................................. 116
  Add an MCU Manually ................................................................................. 116
    Conference Scheduling Requirements ......................................................... 117
  Edit an MCU ............................................................................................... 117
    MCU Settings ............................................................................................ 118
  Delete an MCU Bridge ................................................................................. 120
  View Device Details ..................................................................................... 120
  View Bridge Hardware .................................................................................. 121
  View MCU Services ...................................................................................... 121
  View MCU Conferences .............................................................................. 121
  View MCU Ports .......................................................................................... 122
  View MCU Meeting Rooms .......................................................................... 122
  View MCU Entry Queues ............................................................................. 122
View Bridge Gateway Conferences ................................................................. 123

**Configure Conferencing ................................................................. 124**

**Setting Up Site Topology ................................................................. 125**

- Understanding Site Topology .......................................................... 125
- Managing Sites ...................................................................................... 126
  - View the Graphical Site Topology ...................................................... 126
  - View the Sites List .............................................................................. 127
    - Site Details ....................................................................................... 127
  - Add a Site ......................................................................................... 127
    - Site Settings ................................................................................. 128
  - View Site Information ...................................................................... 131
    - Site Information ............................................................................. 132
  - Assign Locations to a Site ............................................................... 132
  - Edit Site Settings ............................................................................. 133
  - Delete a Site ..................................................................................... 133
- Managing Site Links ............................................................................ 134
  - View the Site Links List .................................................................... 134
    - Site-Links Information ................................................................. 134
  - Add a Site Link .................................................................................. 135
  - Edit a Site Link .................................................................................. 135
  - Delete a Site Link .............................................................................. 135
- Managing Site-to-Site Exclusions .................................................... 136
  - View the Site-to-Site Exclusion List .................................................. 136
  - Add a Site-to-Site Exclusion ............................................................ 136
  - Edit a Site-to-Site Exclusion ............................................................. 136
  - Delete a Site-to-Site Exclusion ......................................................... 136
- Territories ........................................................................................... 137
  - View the Territory List ...................................................................... 137
  - Add a Territory .................................................................................. 137
    - Adding a Territory Settings ............................................................ 137
  - Edit a Territory .................................................................................. 138
  - Delete a Territory .............................................................................. 139
- Network Clouds .................................................................................. 139
  - Multi-tenancy Considerations for Network Clouds ........................... 139
  - View the List of Network Clouds ..................................................... 139
  - Add a Network Cloud ....................................................................... 139
    - Linked Sites Settings ..................................................................... 140
  - Edit a Network Cloud ..................................................................... 140
Contents

Considerations for Anytime Conference Templates ........................................ 158
Configuring Auto-Terminate ......................................................................... 159
Initiating Conference Dial-out ..................................................................... 159

Configuring Conference Settings ................................................................. 160
Specify Conference Settings ...................................................................... 161
Disable Conference Time Warning ............................................................... 161
Automatically Include Conference Creator in Conference ......................... 162
Overbook Dial-in Participants .................................................................... 162
Set the Conference and Chairperson Passcode Length ............................... 162
Customizing Text to Email Notifications ..................................................... 163
  Add Customized Text to Conference Email Notifications .......................... 163
  Edit Customized Text in Email Notifications ............................................. 163

Conference Scheduling .................................................................................. 164

Conference Scheduling Overview ................................................................. 165
  Log into the System .................................................................................. 165
  Conference Scheduler Roles .................................................................... 165
  Scheduling Participants ........................................................................... 166
  Scheduling Bridges and DMA Pool Orders ............................................... 167
    MCU Selection ....................................................................................... 167
    Bridge Scheduling and Reassignment .................................................... 167
    DMA Pool Orders .................................................................................. 167
      Room ID Numbers .............................................................................. 168
      Limitations When Scheduling a Conference on a DMA Pool Order ....... 168
    Conference Templates .......................................................................... 168
  Recurring Conferences .......................................................................... 168
  Anytime Conferences .............................................................................. 169

Conference Scheduling .................................................................................. 170
  Schedule a Conference ............................................................................ 170
  Role Settings ............................................................................................ 172
  Conference Settings ............................................................................... 172
  Configure Advanced Settings .................................................................. 174
    Conference Advanced Settings .............................................................. 175
  Schedule an Anytime Conference ............................................................. 176
  Anytime Conference Role Settings .......................................................... 177
  Scheduling a Point to Point Conference .................................................... 178
  Copy an Existing Conference .................................................................. 178
Edit a Future Conference ........................................... 179
Edit a Participant's Settings ...................................... 179
Participant Settings .................................................. 180
View Scheduling Information for a Conference ................. 181

Managing Conferences and Participants ......................... 182
Working with Conferences ........................................ 182
View All Conferences .............................................. 182
Filter the Conference List ......................................... 183
Delete a Conference ................................................ 184
Export a List of Scheduled Conferences ......................... 184
Managing Active Conferences ..................................... 185
Manage an Active Conference .................................... 185
Participant List Settings ............................................ 185
Write Conference Notes During a Conference ................. 186
Add Additional Participants to an Active Conference ........ 187
Add Guests to an Active Conference ............................. 187
Add a Room to an Active Conference ............................ 188
View a Participant's Video During a Conference ............. 188
Join an Active Conference ........................................ 188
Add a Participant from a Favorites List to an Active Conference ....................................................... 189
Terminate an Active Conference ................................ 189
Managing Participants within an Active Conference .......... 190
Add or Save a Participant to a Favorites List .................... 190
Manage a Participant’s Endpoint During a Conference ........ 190
Managing Participant Settings ..................................... 190
View a Participant's Details During a Conference .......... 191
Participant Device Related Details ................................ 192
Participant Call Related Details .................................. 192

Managing the Guest Book and Favorites Lists ................... 194
Managing the Guest Book ........................................... 194
View the Guest Book ............................................... 194
Guest Book Entries .................................................. 194
Add a Guest to the System Guest Book .......................... 195
Guest Information .................................................... 196
H.323 (IP) Settings .................................................. 196
SIP (IP) Settings ..................................................... 197
H.320 (ISDN) Settings .............................................. 197
Edit a Guest in the Guest Book .................................... 198
Supported Polycom Peripherals .................................................. 244
Managing Third-Party Endpoints .............................................. 245
  Scheduled Provisioning of Third-party Endpoints ...................... 246
Managing Cisco Endpoints ...................................................... 246
  Enable Cisco Endpoints Global Address Book Access .................. 247
  Scheduled Provisioning of Selected Cisco Endpoints .................. 247
  Enable HTTPS for Cisco Endpoints Management ......................... 247
Managing LifeSize Endpoints .................................................. 248
  Enable LifeSize Endpoints Management .................................. 248
  Provisioning LifeSize Passwords .......................................... 248
  Scheduled Provisioning of LifeSize Endpoints ......................... 248
Managing Polycom Software Endpoints ....................................... 250
  Distributing Polycom RealPresence Desktop for Windows Systems ...... 250
  Distribute the Client via an E-mail Link ............................... 250
  Distribute the Client via the Management System ....................... 250
  Distribute the Client via a Desktop Management or Group Policy Object . 250
  Distribute the Client via a ZIP File ................................... 251
  Have users download the client from the Polycom support page .... 251
  Distributing Polycom RealPresence Desktop for MAC Systems ........ 251
  Download the Client from the Polycom Support Page ................. 251
  Distribute the Client for MAC client via an E-mail Link ............ 252
  Distribute the Mac Client via the Management System .............. 252
  Distribute the Mac Client via a .dmg File ............................ 252
Scheduled Endpoint Management ............................................. 253
Scheduled Endpoint Provisioning ............................................. 254
  Supported Endpoints for Scheduled Management ....................... 254
  Scheduled Endpoint Management Settings ............................... 254
    Enable Automatic Registration Synchronization ...................... 254
    Enable Use HTTPs for Cisco Endpoint Management ................... 255
    Use a Common Password for Endpoints ................................ 255
    Disable Common Password for Endpoints ................................ 255
  Creating Scheduled Provisioning Profiles .............................. 256
    Add a Scheduled Provisioning Profile ................................ 256
    Edit a Scheduled Provisioning Profile ................................ 257
    Clone a Scheduled Provisioning Profile ............................... 257
    Delete a Scheduled Provisioning Profile ............................. 257
  Scheduling Endpoints for Provisioning .................................. 257

Polycom, Inc. 15
View a List of Eligible Endpoints ........................................... 258
eligible Endpoints Information ............................................ 258
Schedule Provisioning for Endpoints .................................... 259
Check the Status of a Scheduled Provisioning Update ............. 259
Clear the Status of Scheduled Provisioning ............................ 260
Cancel a Scheduled Provisioning .......................................... 260
Endpoint Fields for Scheduled Provisioning Profiles ............... 260

Dynamic Management ....................................................... 275

Understanding Dynamic Endpoint Management ........................ 276
Supported Polycom Endpoints and Peripherals ......................... 276
Overview of Dynamic Management Setup ................................ 277
Configure Endpoints to use a Provisioning Service ................. 277
Define Endpoint Naming Schemes ....................................... 277
Create Video Endpoint Provisioning Profiles ......................... 277
Create Provisioning Rules ............................................... 278
Create Access Control Lists .............................................. 278
Create Software Updates .................................................. 278
Selective Provisioning of Dynamically Managed RealPresence Group Series Systems ........................................... 278
Dynamically Manage RealPresence Immersive Studio Systems .... 278

Dynamically Updating Endpoint and Peripheral Software ............ 280
Supported Endpoint Types for Dynamic Software Update ............ 280
Software Update Considerations for RealPresence Desktop .......... 281
Creating Dynamic Software Updates for Endpoints ................... 281
List the Serial Numbers for the Endpoints to be Updated ......... 281
Endpoint Serial Number List .............................................. 282
Download the Required Software Package ............................ 282
Request Upgrade Activation Keys ...................................... 283
Upload the Software Update for Dynamic Software Updates ...... 284
Using Dynamic Software Updates ....................................... 284
Decide the Software Version ............................................. 285
View Dynamic Software Update Status .................................. 286
Endpoint List for Dynamic Software Updates .......................... 286
View Software Update Details for an Endpoint ......................... 287
Dynamic Software Details ................................................. 287
View Dynamic Software Update Packages ............................. 288
Dynamic Software Updates .............................................. 289
Set Maintenance Window for Dynamic Software Updates .......... 289
Set up a Trial Dynamic Software Update ........................................ 290
Creating a Local Trial Group .................................................... 290
Create a Trial Software Update Package ...................................... 291
Promote the Trial Software Update Package to Production ............ 291
Delete the Trial Software Update Package .................................... 292
Populate Domain Name for Software Endpoints ......................... 292
Enable Software Endpoints to Save Password .............................. 292
Dynamic Software Updates for Peripherals .................................... 293
View Software Updates for Polycom Touch Controls ..................... 293
Peripheral Software Updates .................................................... 293
Upload Peripheral Software Updates to the RealPresence Resource Manager System 294
Configure Peripheral Updates for Production ............................... 294
Configuring Production Settings .............................................. 295
Configure Peripheral Updates for Trial ........................................ 296
Configuring Trial Settings ....................................................... 296

Using Dynamic Provisioning Profiles ........................................ 298
Set up Dynamic Provisioning Profiles ......................................... 298
Types of Dynamic Endpoint Provisioning Profiles ......................... 298
Working with Provisioning Profiles ......................................... 299
Create a New Provisioning Profile ............................................ 299
Edit a Provisioning Profile ..................................................... 300
Reset a Provisioning Profile ..................................................... 300
Edit a Default Provisioning Profile .......................................... 301
Reset a Provisioning Profile ..................................................... 301
Clone a Provisioning Profile .................................................... 301
Delete a Provisioning Profile ................................................... 301
Network Provisioning Profiles .................................................. 302
Available Settings for a Network Provisioning Profile ................... 302
Admin Config Provisioning Profiles ........................................... 313
Available Settings for Admin Config Provisioning Profiles ............ 314

Creating Dynamic Provisioning Rules ....................................... 318
Prioritizing Provisioning Rules ............................................... 318
Using Rule Conditions ............................................................ 318
Condition Operators .............................................................. 319
Working with Provisioning Rules .............................................. 319
Add a Provisioning Rule .......................................................... 320
Create Provisioning Rule ........................................................ 320
Add a Condition ................................................................. 321
Polycom, Inc. 18

Associate Provisioning Profiles with a Provisioning Rule .............................. 322
View Details of a Provisioning Rule ................................................................. 322
Edit the Priority of a Provisioning Rule .......................................................... 323
Clone a Provisioning Rule .................................................................................. 323
Deactivate a Provisioning Rule ......................................................................... 324
Edit a Provisioning Rule ..................................................................................... 324
Delete a Provisioning Rule ................................................................................ 324
Stop Dynamic Management of an Endpoint ...................................................... 325

Dynamically Managing Endpoint Naming Schemes ........................................... 326
Using Custom Active Directory Attributes ....................................................... 326
Find the Attribute Name to Use ........................................................................ 327
Active Directory Global Service ....................................................................... 327
Define an E.164 Address Scheme ..................................................................... 328
E.164 Numbering Scheme Settings .................................................................... 328
Specify Base Field ............................................................................................ 329
Define an Endpoint Naming Scheme and H.323 Alias ....................................... 330
Endpoint Naming Scheme ................................................................................ 331
H.323 ID Scheme ............................................................................................... 331
Auto-Generate SIP URIs for Dynamically Managed Endpoints ........................... 333
SIP Domain Information .................................................................................... 334

Using Bundled Provisioning Profiles ................................................................. 336
How Bundled Provisioning Works ..................................................................... 336
Considerations for Bundled Provisioning Profiles ............................................. 337
Download a Bundled Provisioning Profile ......................................................... 337
View the List of Bundled Provisioning Profiles .................................................. 337
Edit a Bundled Provisioning Profile ................................................................... 338
Delete a Bundled Provisioning Profile ............................................................... 339
Re-associate Devices with a Different Profile ...................................................... 339
Settings included in a Bundled Provisioning Profile for an HDX ........................ 340
Settings included in a Bundled Provisioning Profile for a RealPresence Group System and Real-Presence Immersive Studio System ................................................................. 347

Using Access Control Lists .............................................................................. 349
Understanding Access Control Lists .................................................................. 349
Planning Implementation of Access Control Lists .............................................. 349
Plan Implementation of Access Control List ....................................................... 350
Using Access Control Lists in a Multi-Tenancy Environment ............................ 350
Add a New Access Control List ......................................................................... 350
Edit an Access Control List .............................................................................. 351
### Scheduling Endpoint Software Updates .......................... 353
- Software Update Considerations for Multi-Tenancy .................. 353
- Creating Scheduled Software Updates for Endpoints .................. 353
  - List the Serial Numbers for the Endpoints to be Updated ........... 354
  - Download the Required Software Package ................................. 354
  - Upload the Software Update for Scheduled Software Updates ....... 355
- Using Scheduled Software Updates ........................................ 356
  - Supported Endpoints for Scheduled Software Updates ............... 356
- Schedule the Software Update for Endpoints .......................... 356
- Scheduled Software Update View .......................................... 357
  - Endpoint List in the Scheduled Software Update View ............... 357
  - Scheduled Software Update Actions .................................... 358
- View Scheduled Software Update Information .......................... 359
- View List of Software Update Packages ................................. 359
- Cancel Software Updates .................................................... 359

### Dynamic Provisioning of Endpoints for SIP Server Integration ........ 361
- SIP Server Authentication Requirements ................................. 361
- Provisioning Endpoints with SIP Server Settings ..................... 362
  - Create Authentication Information for SIP Endpoints ............... 362
  - Import SIP URI Data ...................................................... 362
  - Editing SIP URI Data ..................................................... 363
  - Provision SIP Settings for SIP Server Integration .................. 363
  - Provision Group for Microsoft Skype For Business or Microsoft Office Communications Server Integration ......................... 365
  - Microsoft Directory Considerations .................................. 365
- Using Machine Accounts ..................................................... 365
  - Add a Machine Account ................................................... 366
  - Edit a Machine Account .................................................. 366
  - Machine Account Fields .................................................. 367

### Using Zero-Touch Provisioning .......................... 368
- Configure your DHCP Server .............................................. 368
- Configure Zero Touch Provisioning Settings ........................... 368
- Manually Associate an Endpoint with a Room or User ................. 369
- Enable Calendaring Service ............................................... 369
Dynamically Managing a RealPresence Access Director System .......... 371
Creating a Site for the RealPresence Access Director System .................. 371
Create a RealPresence Access Director Server Provisioning Profile ............... 371
Creating a Network Provisioning Profile for Endpoints .......................... 372
Creating an Admin Config Provisioning Profile ................................. 372
Creating a Provisioning Rule and Associate it with All Related Profiles ........... 373
Creating a User Account for the RealPresence Access Director System ............ 373
Available Settings for RealPresence Access Director Server Provisioning Profile .... 373

Phone Management ........................................................................ 376

Managing Phones ........................................................................ 377
Overview of Phone Management Setup .............................................. 377
Supported Phones and Call Servers .................................................. 377
Managing Phones ................................................................. 379
Automatically Added Phones ...................................................... 380
Configure Automatically Added Phones for Provisioning ....................... 380
Editing Automatically Added Phones ............................................. 381
Add a Phone Manually .......................................................... 381
Edit a Phone ........................................................................ 382
Viewing Phone’s Status .......................................................... 382
Upload Phone Configuration Files ................................................. 383
Change Endpoint Group Association .............................................. 383
Change Configuration Profile Association of Phones .......................... 384
Delete a Phone ...................................................................... 384
Set Active Directory Password .................................................. 384
Control Call Remotely ............................................................... 385
Import Phones Using CSV Files .................................................. 385
   Create a CSV File Containing the Phone Information You Need .......... 385
   Import the CSV File and View the Import Details ......................... 387
Export and Edit Phones ........................................................... 387
Working with Phone Configuration Profiles ...................................... 388
Create a Phone Configuration Profile ............................................ 388
Edit a Phone Configuration Profile .............................................. 389
Copy a Configuration Profile .................................................... 390
Customize the Configuration Profile List ........................................ 390
View CSV Imported Configuration Profiles ......................................... 390
View a Configuration Profile Detail ................................................ 391
Delete a Phone Configuration Profile ............................................ 391
Export Configuration Profiles ................................................................ 391
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Phone Configuration Profile Deployment</td>
<td>392</td>
</tr>
<tr>
<td>Associate Configuration Profiles with Pre-defined Conditions</td>
<td>392</td>
</tr>
<tr>
<td>Reboot Phones</td>
<td>393</td>
</tr>
<tr>
<td>Register Phones to a SIP Server</td>
<td>393</td>
</tr>
<tr>
<td>Monitor Phones Behind Firewall</td>
<td>394</td>
</tr>
<tr>
<td>Working with Resource Files</td>
<td>394</td>
</tr>
<tr>
<td>Upload Resource File</td>
<td>394</td>
</tr>
<tr>
<td>Download Resource File</td>
<td>395</td>
</tr>
<tr>
<td>Delete Resource Files</td>
<td>395</td>
</tr>
<tr>
<td>Refresh Resource Files</td>
<td>395</td>
</tr>
<tr>
<td>Customize the Resource File List</td>
<td>395</td>
</tr>
<tr>
<td>Setting up Phone Software Updates</td>
<td>396</td>
</tr>
<tr>
<td>Upload the Software Update for Phone Software Updates</td>
<td>396</td>
</tr>
<tr>
<td>Customize Software Updates List</td>
<td>397</td>
</tr>
<tr>
<td>Enable System Alerts for New Software Updates on Polycom Hosted Server</td>
<td>397</td>
</tr>
<tr>
<td>Set a Software Update Policy</td>
<td>398</td>
</tr>
<tr>
<td>Managing Polycom® RealPresence® Group Series Via Polycom® Trio™</td>
<td>398</td>
</tr>
<tr>
<td>Upload the Software Update for Group Series Endpoints</td>
<td>399</td>
</tr>
<tr>
<td>Working with CUCM</td>
<td>399</td>
</tr>
<tr>
<td>Configuring Cisco Unified Communications Manager</td>
<td>400</td>
</tr>
<tr>
<td>Start the Cisco AXL Web Service</td>
<td>400</td>
</tr>
<tr>
<td>Creating a User for the RealPresence Resource Manager Integration</td>
<td>400</td>
</tr>
<tr>
<td>Enabling Auto Discovery of RealPresence Resource Manager through DHCP</td>
<td>402</td>
</tr>
<tr>
<td>Creating Phone Configuration Profiles</td>
<td>402</td>
</tr>
<tr>
<td>Configuring the CUCM as a SIP server (Optional)</td>
<td>402</td>
</tr>
<tr>
<td>Customizing Digest User Password</td>
<td>402</td>
</tr>
<tr>
<td>Integrating with a Cisco Unified Communications Manager</td>
<td>402</td>
</tr>
<tr>
<td>Add a Cisco Unified Communications Manager</td>
<td>402</td>
</tr>
<tr>
<td>Synchronize with the Cisco Unified Communication Manager</td>
<td>403</td>
</tr>
<tr>
<td>Configure Your Phone Management Settings</td>
<td>404</td>
</tr>
</tbody>
</table>

**User Management** ......................................................................... 406

**Working with Users** ................................................................... 407

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Users</td>
<td>407</td>
</tr>
<tr>
<td>Enterprise Users</td>
<td>407</td>
</tr>
<tr>
<td>Managing Local Users</td>
<td>408</td>
</tr>
<tr>
<td>Add a Local User</td>
<td>408</td>
</tr>
<tr>
<td>User Information</td>
<td>409</td>
</tr>
<tr>
<td>Import Local Users</td>
<td>410</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Sample CSV file of User Information</td>
<td>411</td>
</tr>
<tr>
<td>Troubleshooting the Import Details File</td>
<td>412</td>
</tr>
<tr>
<td>Handle the User Accounts with Password Lost</td>
<td>412</td>
</tr>
<tr>
<td>Updating Local Users by Import</td>
<td>412</td>
</tr>
<tr>
<td>Delete a Local User</td>
<td>413</td>
</tr>
<tr>
<td>Managing Users</td>
<td>414</td>
</tr>
<tr>
<td>Search for a User</td>
<td>414</td>
</tr>
<tr>
<td>View User Information</td>
<td>414</td>
</tr>
<tr>
<td>User Information Details</td>
<td>414</td>
</tr>
<tr>
<td>Edit a User</td>
<td>415</td>
</tr>
<tr>
<td>Assign Users to Manage an Area(s)</td>
<td>416</td>
</tr>
<tr>
<td>Enable/Disable Users</td>
<td>417</td>
</tr>
<tr>
<td>Unlock a User Account</td>
<td>417</td>
</tr>
<tr>
<td>Clear Orphan Active Directory Users/Rooms</td>
<td>417</td>
</tr>
<tr>
<td>Managing Dial String Reservations for Users</td>
<td>418</td>
</tr>
<tr>
<td>Export User Aliases</td>
<td>418</td>
</tr>
<tr>
<td>Importing User Aliases</td>
<td>419</td>
</tr>
<tr>
<td>SIP Format:</td>
<td>419</td>
</tr>
<tr>
<td>H323 Format:</td>
<td>420</td>
</tr>
<tr>
<td>Importing User Aliases</td>
<td>421</td>
</tr>
<tr>
<td>Working with Management Roles and Permissions</td>
<td>423</td>
</tr>
<tr>
<td>Understanding User Roles</td>
<td>423</td>
</tr>
<tr>
<td>Managing User Roles</td>
<td>424</td>
</tr>
<tr>
<td>View the List of User Roles</td>
<td>424</td>
</tr>
<tr>
<td>Add a User Role</td>
<td>424</td>
</tr>
<tr>
<td>Adding Role Settings</td>
<td>424</td>
</tr>
<tr>
<td>Edit Permissions for a User Role</td>
<td>425</td>
</tr>
<tr>
<td>Delete a User Role</td>
<td>425</td>
</tr>
<tr>
<td>View the Groups and Users Associated with a User Role</td>
<td>426</td>
</tr>
<tr>
<td>Assigning Roles to Enterprise Users</td>
<td>426</td>
</tr>
<tr>
<td>Default System Roles and Permissions</td>
<td>426</td>
</tr>
<tr>
<td>Scheduler Roles, Responsibilities, and Menus</td>
<td>428</td>
</tr>
<tr>
<td>Operator Role, Responsibilities, and Menus</td>
<td>429</td>
</tr>
<tr>
<td>Device Administrator Role, Responsibilities, and Menus</td>
<td>429</td>
</tr>
<tr>
<td>Auditor Role, Responsibilities, and Menus</td>
<td>429</td>
</tr>
<tr>
<td>Administrator Role, Responsibilities, and Menus</td>
<td>430</td>
</tr>
<tr>
<td>Customized Roles and Responsibilities</td>
<td>430</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Working with Groups</td>
<td>432</td>
</tr>
<tr>
<td>Local Groups</td>
<td>432</td>
</tr>
<tr>
<td>Enterprise Groups</td>
<td>432</td>
</tr>
<tr>
<td>Managing Groups</td>
<td>432</td>
</tr>
<tr>
<td>Add a Local Group</td>
<td>432</td>
</tr>
<tr>
<td>User Group Settings</td>
<td>433</td>
</tr>
<tr>
<td>Import Enterprise Groups</td>
<td>433</td>
</tr>
<tr>
<td>Edit a Group</td>
<td>434</td>
</tr>
<tr>
<td>Delete a Group</td>
<td>434</td>
</tr>
<tr>
<td>Managing Meeting Rooms</td>
<td>436</td>
</tr>
<tr>
<td>View the Rooms List</td>
<td>436</td>
</tr>
<tr>
<td>Search for a Room</td>
<td>436</td>
</tr>
<tr>
<td>Add a Local Room</td>
<td>437</td>
</tr>
<tr>
<td>Room Information</td>
<td>437</td>
</tr>
<tr>
<td>Add an Enterprise Room</td>
<td>438</td>
</tr>
<tr>
<td>Edit a Room</td>
<td>439</td>
</tr>
<tr>
<td>Delete a Room</td>
<td>439</td>
</tr>
<tr>
<td>System Configuration</td>
<td>440</td>
</tr>
<tr>
<td>Securing the System</td>
<td>441</td>
</tr>
<tr>
<td>Managing Security Baselines</td>
<td>441</td>
</tr>
<tr>
<td>Create a Security Baseline</td>
<td>441</td>
</tr>
<tr>
<td>View a Security Baseline</td>
<td>442</td>
</tr>
<tr>
<td>Edit a Security Baseline</td>
<td>442</td>
</tr>
<tr>
<td>Delete a Security Baseline</td>
<td>442</td>
</tr>
<tr>
<td>Apply Security Baseline</td>
<td>443</td>
</tr>
<tr>
<td>Audit Your System Against a Security Baseline</td>
<td>443</td>
</tr>
<tr>
<td>Audit Baseline Results</td>
<td>443</td>
</tr>
<tr>
<td>Configure Secure Communication</td>
<td>444</td>
</tr>
<tr>
<td>Secure Communication Protocols</td>
<td>444</td>
</tr>
<tr>
<td>Configure TLS Settings</td>
<td>444</td>
</tr>
<tr>
<td>TLS Settings</td>
<td>445</td>
</tr>
<tr>
<td>Configure System Hardening</td>
<td>447</td>
</tr>
<tr>
<td>System Hardening</td>
<td>447</td>
</tr>
<tr>
<td>Session Security and User Access</td>
<td>447</td>
</tr>
<tr>
<td>Change the System User Interface Timeout and Number of Sessions</td>
<td>448</td>
</tr>
<tr>
<td>Session Management Settings</td>
<td>448</td>
</tr>
<tr>
<td>Disable Linux Console Access</td>
<td>448</td>
</tr>
</tbody>
</table>
Enabling and Editing Log in Banners .............................................. 449
  Enable Banner ........................................................................ 449
  Edit Banner ........................................................................... 449
Set Local Account Lockout and Timeout ........................................... 449
  User Account Configuration Settings ........................................... 450
Using Whitelist for IP Access .......................................................... 450
  Create a Whitelist to Manage Access ............................................ 450
  Disable Management Access Settings .......................................... 451
Set Sensitive Information Disclosure ................................................. 451
Set Password Requirements ............................................................ 451
  Password Requirement Settings .................................................. 451
Reset System Passwords ................................................................. 452
Encryption .................................................................................. 453
Security Certificates ..................................................................... 454
  How Certificates Work ............................................................... 454
  Accepted Certificates ............................................................... 454
  Certificate Signing Requests ...................................................... 456
    Requirements for Certificate Signing Request .......................... 456
    Create a Certificate Signing Request ....................................... 458
      Certificate Request Data ....................................................... 459
Installing Certificates .................................................................. 460
  Install a Certificate .................................................................. 460
  View Certificates and Certificate Details ...................................... 461
    Certificate Management Information ...................................... 461
    Certificate Details .................................................................. 462
Removing Certificates .................................................................. 462
  Remove a Trusted Root CA’s Certificate .................................... 463
  Remove a Signed Certificate and Revert to Default Self-Signed Certificate ................................................. 463
  Regenerate a Default Self-Signed Certificate ............................. 464
  Revert to a Legacy VVX Certificate ............................................. 464
OCSP Settings ............................................................................ 464
Configuring Multi-Tenancy ............................................................... 466
  Planning For Multi-Tenancy ......................................................... 466
  Working within a Multi-Tenancy Environment .............................. 467
    User Roles within a Multi-Tenancy Environment ...................... 467
      System Roles ........................................................................ 467
      Area Roles ........................................................................... 467
      Area Conference Participants ................................................ 468
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Address Books</td>
<td>468</td>
</tr>
<tr>
<td>Area User Groups</td>
<td>469</td>
</tr>
<tr>
<td>Area Users, Rooms, and Associated Endpoints</td>
<td>469</td>
</tr>
<tr>
<td>Area Conference Guests</td>
<td>469</td>
</tr>
<tr>
<td>Using the Common Pool in a Multi-Tenancy Environment</td>
<td>470</td>
</tr>
<tr>
<td>Area Conference Templates</td>
<td>470</td>
</tr>
<tr>
<td>Configure Areas</td>
<td>470</td>
</tr>
<tr>
<td>Create Areas for Tenants</td>
<td>471</td>
</tr>
<tr>
<td>Setting up Area Management</td>
<td>471</td>
</tr>
<tr>
<td>Managing the Area with System Roles</td>
<td>471</td>
</tr>
<tr>
<td>Managing the Area with Area Roles</td>
<td>471</td>
</tr>
<tr>
<td>Assigning Resources to an Area</td>
<td>472</td>
</tr>
<tr>
<td>Resources Belong to One or No Area</td>
<td>472</td>
</tr>
<tr>
<td>Resources Belong to One or More Areas (or no Area)</td>
<td>472</td>
</tr>
</tbody>
</table>

**Adding Users to An Area**                                        | 472  |

- Configuring Site Topology                                             | 473  |
- Associating Billing Codes with Conferences                           | 473  |
  - Add a New Billing Code                                              | 474  |
  - Delete a Billing Code                                               | 474  |
  - Associating a Billing Code with a Conference                        | 475  |
- Viewing Billing Code Information                                       | 475  |

**Managing Areas**                                                    | 476  |

- Enable Areas                                                          | 476  |
- Add an Area                                                           | 476  |
- Edit an Area                                                         | 477  |
- Viewing All Areas                                                     | 477  |
- View Information for a Specific Area                                 | 478  |
- Remove an Area                                                       | 478  |
  - Move the Contents of an Area                                       | 478  |
  - Deleting an Area and its Resources                                 | 479  |
- Customizing the Area Logos (system and CMA Desktop) for the Area     | 480  |
- Customize the System Log for an Area                                 | 480  |
- Customize the CMA Desktop Logo                                       | 480  |

**System Redundancy**                                                  | 481  |

- How Redundancy Works                                                 | 481  |
- Configuration Considerations for Redundancy                           | 482  |
- Interoperability Considerations for Redundancy                        | 482  |
- Local versus Geographic Redundancy                                   | 483  |
Managing a Redundant System ................................................. 483
Manually Failover to a Redundant Server ............................... 483
Track System Failovers .................................................... 484
Failover Information ....................................................... 484
Discontinue Redundancy ................................................. 484
Restore Redundancy ....................................................... 485

Configuring Local System Redundancy ................................. 486
Optional: Perform a System Backup .................................... 486
Ensuring the Servers Can Communicate ............................... 486
Network Configuration Requirements on Both Servers .......... 486
Enable the Root User Login and SSH Access ..................... 487
Optional: Change the Redundant Interface IP Address .......... 487
Network Interface IP Address ........................................... 487
Configure the System for Redundancy ................................ 488
IP Settings for Local Redundant Configuration ..................... 488
License a Local Redundant System ..................................... 489
Provisioning Considerations ............................................ 489

Geographic System Redundancy .......................................... 491
Network Requirements for a Geographic Redundant System .... 491
Optional: Perform a System Backup .................................... 491
Perform Network Configuration on Both Servers ................. 491
Enable the Root User Login ............................................. 492
Configure DNS for the Redundant Servers ......................... 492
Configure the System for Redundancy ................................ 492
IP Settings for Geo-redundant Configurations ..................... 493
License a Geographic Redundant System ......................... 493
Provisioning Considerations ............................................ 494

System Maintenance ....................................................... 495
System Management and Maintenance ................................. 496
Administrator Responsibilities ........................................ 496
Administrative Best Practices .......................................... 496
Auditor Responsibilities ................................................. 497
Auditor Best Practices .................................................. 497
Recommended Regular Maintenance ................................. 497
Tracking System Alerts .................................................. 497
Creating Backup Archives .............................................. 498
General System Health and Capacity Checks ........................................ 498
Exporting CDR ................................................................. 498

System Reports ................................................................. 499
View Site Statistics Report ....................................................... 499
Site Statistics ................................................................. 499
View Site Link Statistics Report ............................................... 500
Site Link Statistics ............................................................ 500
Call Detail Record Report Administration .................................. 501
  Modify the CDR Retention Period ......................................... 501
  Schedule Archives of the CDR Report .................................... 501
  Report Administration Settings ............................................ 501
View Endpoint Usage Report .................................................. 502
Available Endpoint Usage Report ............................................ 503
Generate Endpoint Usage Report Properties ............................... 504
Summary CDR Report .......................................................... 504
Detail CDR Report ............................................................. 504
Generate Network Device Usage Report ..................................... 507
Create Conference Usage Report ............................................. 507
Conference Usage Report ...................................................... 508
Create Conference Type Report .............................................. 508
Conference Type Report ....................................................... 509

RealPresence Resource Manager System SNMP ......................... 511
SNMP Framework ............................................................. 511
SNMP Notifications .......................................................... 511
SNMP Versions ................................................................. 512
Configuring SNMP ............................................................. 512
  Enable the SNMP Agent ..................................................... 513
    SNMP Agent Settings .................................................... 513
  Add an SNMP Notification Agent ........................................ 514
    Add Notification Agent Properties .................................... 514
  Add a Security User (SNMP v3 only) .................................... 515
    Add Notification User Properties ..................................... 515
  Enable SNMP for an Instance ............................................. 516
    Network Device SNMP Configuration .................................. 516
Download MIBs ................................................................. 517
Polycom RealPresence Resource Manager MIBs .......................... 518
Configuring Alert Settings .............................................................. 520
   Setting Up Remote Alerts .......................................................... 520
   Set Up System Generated E-mail Account ..................................... 520
   Enable RealPresence Resource Manager System Remote Alerts .......... 521
   Set RealPresence Resource Manager System Remote Alert Level Settings .......................................................... 521
   Set RealPresence Resource Manager System Alert Threshold Settings .......................................................... 521
   Set Endpoint Alert Level Settings .............................................. 522
      Endpoint Alert Level .............................................................. 522
   Configuring Remote Alert Profiles ............................................. 523
      Add a Remote Alert Profile ...................................................... 523
      Supported Device Types for Remote Alerts ................................ 525
      Associate a Remote Alert Profile With a User ............................. 526
      Edit a Remote Alert Profile .................................................... 526
      Disable a Remote Alert Profile .............................................. 527
      Delete a Remote Alert Profile .............................................. 527
   Disable System Remote Alerts ................................................... 527
   Viewing and Deleting Network Device Alerts .................................. 527
      Viewing Alerts ................................................................. 528
      Alert Types ................................................................. 528
      Delete Active Alert .......................................................... 532
      View Endpoint Event Status .................................................. 532

System Backup and Recovery ...................................................... 533
   Creating System Backups .......................................................... 533
   Create an Automatic System Backup .......................................... 533
      FTP of Auto System Backup Settings ...................................... 534
   Create a System Backup Manually ............................................. 534
   Restoring the System .............................................................. 535
      Restore to Factory Default Image ........................................... 536
      Restore from a Backup Archive ............................................. 536

System Maintenance and Troubleshooting .................................... 538
   System Log Overview ............................................................. 538
   Available System Logs ........................................................... 539
   Managing Locally Stored System Logs ....................................... 539
      View Locally Stored System Log Files ..................................... 539
      Change Logging Level for Locally Stored Logs ........................... 540
      Local Settings of Log Files ................................................ 540
   Download Locally Stored Log Files .......................................... 541
   Roll Locally Stored Log Files .................................................. 541
Instance Management ................................................................. 561
  Adding a New Virtual Instance ........................................... 561
  Adding an Existing Virtual Instance ..................................... 562
  Delete Uploaded Images ..................................................... 562
Service Integration .............................................................. 563
vCenter Permissions ............................................................ 563
  VMware APIs Used by RealPresence Resource Manager .......... 563
Instance Management .......................................................... 564
  Two Methods for Adding VM Instances in a vCenter ............ 564
Monitoring vCenter Resources .............................................. 565
Recommendations ............................................................... 566

Supported Ciphers ............................................................. 567
Getting Started

Polycom® RealPresence® Resource Manager is an integrated scheduling and management platform for endpoints and video conferencing infrastructure management.
Polycom RealPresence Resource Manager Overview

RealPresence Resource Manager is an integrated scheduling and management platform for endpoints and video conferencing infrastructure management. In particular, it functions as the management and licensing platform for Polycom® RealPresence Clariti™.

RealPresence Resource Manager Features and Capabilities

RealPresence Resource Manager can schedule and monitor conferences, manage and monitor endpoints, and manage and control licenses.

Video Infrastructure Management

- Network device management. You can view and manage all of your Polycom video conferencing network devices from a single interface. Network device management and system monitoring and management including network typology by geography and visual alarm reporting.
- Configuration for service groups. You can create a service group of all the Polycom network devices within your video environment. This allows you to configure settings on a service group level.
- Licensing management. RealPresence Resource Manager system acts as the licensing interface between the Polycom Licensing Center and your RealPresence Clariti products.
- Solution monitoring for network devices. Monitor all the network devices within your video infrastructure environment.
- Multi-tenancy support.

Video Endpoint and Phone Management

- Video endpoint management, including provisioning, updating, and troubleshooting.
- Video endpoint provisioning enables you to edit endpoint settings for the endpoints registered to the RealPresence Resource Manager. You can take advantage of dynamic (automatic) provisioning for Polycom endpoints, based on provisioning rules. For legacy and third-party endpoints, you can manually schedule provisioning profiles to be sent at intervals you define.
- Dynamic software updates for dynamically managed Polycom endpoint systems and scheduled software updates for third-party and legacy endpoints.
- Phone management includes provisioning, updating, and troubleshooting.
Conference Scheduling

- Conference scheduling and monitoring on both RealPresence Resource Manager RealPresence Collaboration Server and the Polycom® RealPresence® DMA® systems (when integrated with the RealPresence Resource Manager system).
- Advanced routing to distribute audio and video calls across multiple conferencing platforms (MCUs), creating a single seamless resource pool, when integrated with a Polycom RealPresence DMA system.

Directory Services

- Directory and user management including address books and presence. Integration with an enterprise directory for user management.
- 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.

Managing Bandwidth for RealPresence DMA

The RealPresence Resource Manager system manages the bandwidth between sites and the bandwidth for calls that it schedules within the gatekeeper region it services. The sites and bandwidth management is only possible with a RealPresence DMA system.

Users with administrator permissions can create bandwidth management policies by setting the following limits. The RealPresence 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 General Info, 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. It is inherited from the conference template. You can achieve granularity of bandwidth management by the following ways:
    - Creating a variety of scheduling roles.
    - Creating a variety of conference templates with different conference speeds.
    - Associating different scheduling roles with different templates.
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 RealPresence Resource Manager system may reduce bandwidth or fail a call if the requested bandwidth isn’t 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 RealPresence 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’ll 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 an Admin Config provisioning profile. For endpoints operating in scheduled management mode, these values can be provisioned with a scheduled provisioning profile or modified at the endpoint itself.

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

Session Border Control Integration

Integrate with session border control systems, which enable video conferencing across firewalls.

Redundant Configuration

An optional high-availability, redundant management server configuration.

Programmatic Access through API

Optional programmatic access through Application Programming Interfaces (APIs).

Navigating the RealPresence Resource Manager System

You can learn the basic tasks of working in a RealPresence Resource Manager system.

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

- No shared directory services
Polycom RealPresence Resource Manager Overview

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

Log In to the System

To log in to the RealPresence Resource Manager web interface, you need the IP address or host name of the RealPresence Resource Manager system server and your user name, password, and domain.

For security reasons, don’t save your user name and password.

User with Admin role will be locked for 1 minute after three (default) failed attempts, while other users follow the rules of failed login that the Admin sets.

To log in to the system:

1. Open a browser and 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 Continue.
   - If you see a login banner, click Accept to accept the terms and continue.
   If you can't connect to the system, there may be certificate issues. Contact your RealPresence Resource Manager system administrator.

2. When the system Log In screen appears, enter your user name and Password. If you're logging in with your enterprise directory account, include your domain (domain/username). Local users don’t have to include a domain.

3. If necessary, select a different language from the bottom of the login page.

4. Click Login.

Because the RealPresence Resource Manager system is a role-based system, you see only the pages and functions available to your system roles.

If you log in as an administrator, you see the RealPresence Resource Manager system Dashboard.

Related Topics

Working with Management Roles and Permissions
Set Local Account Lockout and Timeout

System Dashboard

When you log in to the RealPresence Resource Manager system with the Administrator role and permissions, the system first displays the system Dashboard. Use the system Dashboard to view information about system health and activity levels.
The system **Dashboard** displays data in an array of charts, forms, data grids, and other graphical displays. You can modify your system **Dashboard** layout by moving, closing, and restoring panes. Also note that your changes to the system **Dashboard** are remain but between logouts and logins.

### Dashboard Panes

Within the **Dashboard**, you can customize the panes you see by selecting the following panes under the **Add Panes** drop-down list.

#### Today’s Scheduled Conferences

The **Today’s Scheduled Conferences** pane displays information about the scheduled conferences managed by the RealPresence Resource Manager system. For the current day (starting at 0:00 and ending at 24:00), it displays:

- The number of **Total** scheduled conferences.
- The number of **Ongoing** scheduled conferences.

When the cursor stays on the bar, it displays:

- The number of scheduled conferences that were **Completed** that day.
- The number of scheduled conferences that are **Ongoing** at the current time.
- The number of scheduled conferences that are yet to occur (**Future**).

#### Endpoint Number

The **Endpoint Number** pane displays the number of endpoints registered with the RealPresence Resource Manager system. It displays the total endpoint number and the online endpoint number.

The bar displays the online and offline number of the registered endpoints. The green part is the number of online endpoints. The gray part is the offline number of the endpoints.

#### CPU/Memory/Disk

This pane displays general information about the current CPU, memory, and disk usage of the system. When the CPU and memory usage is under 75%, the color is green. When the usage is between 75% and 90%, the color is yellow. When the usage is over 90%, the color is red.

#### Users

This pane displays:

- The total number of local users, enterprise users (with endpoints associated), and rooms.
- The number of the rooms.

When the cursor stays on the bar, it displays:

- The number of local users, enterprise users (with endpoints associated), and rooms.
- The number of guests.
Today’s Adhoc Conferences

The Today’s Adhoc Conferences pane displays information about the adhoc conferences started by video endpoints registered to the RealPresence Resource Manager system. For the current day (starting at 0:00 and ending at 24:00), it displays:

- The number of Total adhoc conferences.
- The number of adhoc conferences that are Ongoing at the current time.

When the cursor stays on the bar, it displays:

- The number of adhoc conferences that were Completed for the current day.
- The number of adhoc conferences that are Ongoing at the current time.

Adhoc conferences that take place on MCUs that are managed by the RealPresence DMA system cannot be accurately monitored by the RealPresence Resource Manager. Monitoring information will be incorrect and inconsistent.

Hardware Usage

This pane displays the temperature, battery, and cooling fan status. You can only see this pane on the appliance edition.

- Temperature—Temperature status information provided by the Polycom-branded Dell server agent through its MIB.
- Battery Status—Battery status information provided by the Polycom-branded Dell server agent thought its MIB.
- Cooling Fan—Fan status information provided by the Polycom-branded Dell server agent thought its MIB.

Endpoint Type

The system enables you to add multiple Endpoint Type panes. When you add an Endpoint Type pane, you can give the pane a meaningful name and select to display the endpoints by type, by site, or by endpoint group. The pie chart displays up to the six endpoint types. When there are more than six endpoint types by type, site or groups, the pie chart displays the top five endpoint types.

- By Site: The site name and endpoint number are displayed.
- By Endpoint Type: The endpoint type and endpoint number are displayed.
- By Endpoint Group: The endpoint group name and endpoint number are displayed.

You can save the pane and create others as needed. You can also reconfigure an Endpoint Type pane using the configuration tool.

When the cursor stays on a specific type of endpoint on the meter, the endpoint name and number are displayed.

Site Map

This pane displays the site topology. If there are over 500 sites, the system does not display the Site Map pane. See Setting Up Site Topology for details.
Service Groups
This pane displays the service groups. See Managing Service Groups for details.

Today's Conferences Statistics
Select Scheduled Conference, Ad-hoc conference, or Both from the Type drop-down list to display the information about:

- Scheduled conferences managed by the RealPresence Resource Manager system. For the current day (starting at 0:00 and ending at 24:00), it displays a bar chart that displays time on the linear axis plotted against the number of scheduled conferences on the horizontal axis.
- Ad hoc conferences started by video endpoints registered to the RealPresence Resource Manager system. For the current day (starting at 0:00 and ending at 24:00), it displays a bar chart that displays the number of ad hoc conferences (vertical axis) plotted against time of day (horizontal axis).

System Info
This pane displays general information about the system, including:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Time</td>
<td>Displays the current time of the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Last JServer Start Time</td>
<td>The last time when JServer started.</td>
</tr>
<tr>
<td>Server Address</td>
<td>The IP address of the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The RealPresence Resource Manager system version number.</td>
</tr>
<tr>
<td>Hardware Version</td>
<td>The Dell hardware version of the system.</td>
</tr>
<tr>
<td></td>
<td>• Rev D, R620</td>
</tr>
<tr>
<td></td>
<td>• Rev E, R220</td>
</tr>
<tr>
<td></td>
<td>• Rev F, R630</td>
</tr>
<tr>
<td></td>
<td>• Rev G, R230</td>
</tr>
<tr>
<td>Remote Access</td>
<td>Displays whether or not Remote Desktop Connection is enabled.</td>
</tr>
<tr>
<td>Provisioning in Progress</td>
<td>Displays the number of scheduled endpoint provisioning processes that are currently underway.</td>
</tr>
<tr>
<td>Software Updates in Progress</td>
<td>Displays the number of scheduled endpoint software update processes that are currently underway.</td>
</tr>
<tr>
<td>Failed Logins (last 24 hours)</td>
<td>The total number of Failed Logins for Active Directory users in the last 24-hour period.</td>
</tr>
</tbody>
</table>

Endpoints
The system enables 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.

Each **Endpoints** pane can list up to 500 endpoints.

**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**

**Precall Status**

The **Precall 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 precall 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>
<tr>
<td>Ready to Launch</td>
<td>Displays the subset of conferences that are scheduled to start in the next 10 minutes and that have passed the resource tests that the system executes before launching a conference.</td>
</tr>
<tr>
<td>Ready to Launch with Device in Call</td>
<td>Displays the subset of conferences that are scheduled to start in the next 10 minutes and that have passed the resource tests but that still have one or more devices in another call.</td>
</tr>
<tr>
<td>NOT Ready to Launch</td>
<td>Displays the subset of conferences that are scheduled to start in the next 10 minutes but that haven’t yet passed the resource tests. Also displays the conferences that aren’t ready to launch.</td>
</tr>
</tbody>
</table>

**MCU Status**

The system enables you to add multiple **MCU Status** panes so you can create a pane for all or individual MCUs registered with the RealPresence 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:

If your system has areas enabled, you’ll be able to view only the MCUs that belong to areas that you’ve been assigned to manage.
Polycom RealPresence Resource Manager Overview

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 for all of the registered MCUs.</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 total number of active conferences being hosted by all of the registered MCUs.</td>
</tr>
</tbody>
</table>

Errors Displays the number of alarms on the MCU.

Warnings Displays the number of conferences that are active on the MCU at the current time.

Active Conferences Displays the number of active conferences currently being hosted by the MCU.

Number of Audio Ports Displays the number of dedicated audio ports configured on the MCU.

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 RealPresence Resource Manager system.

In addition, the MCU Status pane identifies when the monitored MCU is experiencing alert conditions.

Users Logged In

The Users Logged In pane displays the type and number of users that are currently logged in to the system. A sparkline presents the number of logins over time (30 minutes total; updated every 5 minutes so there are six data points on the sparkline) for each user type.

The system identifies three user types by their permissions: Administrators, Operators, andSchedulers. Note that these three user types aren’t 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. See Working with Management Roles and Permissions for details.

Polycom, Inc.
Redundancy Status

The Redundancy Status pane displays information about the RealPresence 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 isn’t configured for redundancy, the value will be No.
- The IP address of the Active Server.
- The IP address of the Backup Server.

Video Endpoint Licenses (Non-Clariti Only)

The Video Endpoint Licenses pane displays:

- The total number of video licenses available on the system
- The number of free video licenses. When the cursor stays on the gray part of the bar, it also shows the number of free licenses.
- Used video licenses: when the cursor stays on the blue part of the bar, it shows the number of used licenses.

Audio and/or Content Endpoint Licenses (Non-Clariti Only)

The Audio and/or Content Endpoint Licenses pane displays:

- The total number of phone and content device (Pano) licenses available on the system.
- The number of free audio/content licenses. When the cursor stays on the light blue part of the bar, it also shows the number of free licenses.
- Used audio/content licenses: when the cursor stays on the blue part of the bar, it shows the number of used licenses.

CUCM

The CUCM pane displays the information about the integrated Cisco Unified Communication Manager information.

DMA

The DMA pane displays the service information about the integrated RealPresence DMA system. If the RealPresence Resource Manager system is integrated with a RealPresence DMA local cluster or super cluster, the DMA pane doesn’t display the RealPresence DMA nodes status.

View Alerts

The triangle in the top-right corner of the Dashboard shows the overview of the system alerts. The color of the triangle shows the highest level of the existing alert. For example, if there’s a critical alert, the triangle is red. It also shows the total number of the system alerts.
To view the alerts:

1. Click Alert in the top-right corner of the Dashboard.
2. View the alerts on the Alert > Alert View page.

**Field Input Requirements**

If you work in a language other than English, be aware that some RealPresence Resource Manager fields may accept only ASCII or extended ASCII characters.

**Searching in a List**

In the RealPresence Resource Manager system, 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. You can search endpoints by Name, IP address, Dial String, Site, and other keywords.

In general, most text filter fields are ASCII only and the RealPresence Resource Manager search function is a case-insensitive, substring search. That means when you enter a search string, the RealPresence Resource Manager looks for that string wherever it occurs (beginning, middle, or end) in the word or number.

**Related Topic**

LDAP Searches

**Download Software Packages**

You can download the software packages of RealPresence Desktop for Windows and Mac or Polycom File Verification Utility directly from the system web interface.

To download software packages:

1. Click Username > Download at the top-right corner of the page.
2. Click the Download button of the software that you want to download. You can download:
   - Polycom RealPresence Desktop for Windows
   - Polycom RealPresence Desktop for Mac
   - Polycom File Verification Utility
     - See Backup and Delete Audit Files for details on how to use Polycom File Verification Utility.

**Related Topic**

Backup and Delete Audit Files
Change a Password

The RealPresence Resource Manager system administrator manages the system password for local users, while Microsoft Active Directory for enterprise users.

For local users, the system administrator can set password requirements, for example, password length and password age. Microsoft Active Directory can do the same for enterprise users as well.

To change your system password:

1. Click Username > Change Password in the top-right corner of the page.
2. Enter your Old Password.
3. Enter a password to the New Password and Confirm Password fields.
4. For users with admin role, you can select the check box on the bottom of the dialog to apply the same password to the admin users that you specified when adding the following servers as network instances:
   - RealPresence DMA
   - RealPresence Collaboration Server
   - Web Suite Services and Experience Portal

   ![Warning](image)

   This operation doesn’t apply to RealPresence DMA and RealPresence Collaboration Server with service integrated.

5. Confirm the new password and click OK.

Log Out of the System

You can log out of the system at any time.

To log out of the RealPresence Resource Manager system:

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

Restart or Shut Down a System

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

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

- Use the Shutdown option on the Admin > Maintenance > Troubleshooting Utilities page 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 same page when you must cycle the RealPresence Resource Manager system for some reason; for example, if the system locks up or loses connection with Active Directory.

If you have access to the RealPresence Resource Manager user interface, you can also stop future scheduled conferences from starting automatically and wait for active conferences to end before performing an orderly shutdown or restart of the system.

**To restart or shut down the system:**

1. **(Optional) To stop future scheduled conferences from starting before you perform the restart or shutdown:**
   a. Go to Dashboard.
   b. Monitor the Today’s Scheduled Conferences section to determine when all active conferences are completed.

2. Go to Admin > Maintenance > Troubleshooting Utilities 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’s initiating a failover.

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

**Shut Down the System in Emergency**

Only perform an emergency shutdown when necessary. After an emergency shutdown, a system battery may continue to cache information until the battery runs out. In this case, the system enters an error state and you must recover the system.

**To shut down the system in emergency:**

1. Shut down the system in one of the following ways:
   - Press and hold the power switch on the RealPresence Resource Manager system server.
   - Pull the system power cord.

2. Recover the system.
   a. Connect a keyboard and monitor to the RealPresence Resource Manager system.
   b. Boot the system to clear the error message. Then the system can begin recovery.
Network Configuration

Configure your network settings before you start to use RealPresence Resource Manager to manage your devices or conferences.

Configuring your DNS Server

You need to configure DNS server to discover the RealPresence Resource Manager system automatically. This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager system to:

- resolve queries for the RealPresence Resource Manager by the RealPresence Resource Manager’s host name or IP address.
- dynamically manage endpoints (which includes dynamic provisioning, dynamic software update, and presence).

Adding DNS SRV Record for RealPresence Resource Manager System Services

To resolve queries to the RealPresence Resource Manager system using the system's host name or IP address, you must configure the DNS server. Polycom recommends you to configure the DNS server using the system's fully qualified domain name (FQDN) to ensure that client systems running RealPresence Desktop and RealPresence Mobile 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 dynamic provisioning, dynamic software updates, and presence), 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
```

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.

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).
Edit Network Settings

You can edit the network settings to change the basic network information for the RealPresence Resource Manager system. Some networks setting changes require a restart, such as updating the IP address or changing the subnet mask.

Some network changes also require you to install a new security certificate or certificate chain. When you use certificates, you must request and install a new certificate or certificate chain if you change the system name, DNS domain name or switch from supporting single to multiple IP protocols or vice versa.

To edit network settings:

1. Go to Admin > Server Settings > Network.
2. Configure the settings on the Service Interface tab, as necessary.
3. Click Save Settings.
   - If you change the IP address, the system prompts you to restart the RealPresence Resource Manager system. We also recommend that you restart the system if you change the subnet mask.
4. As required, restart the system.
   - Ensure to connect RealPresence Resource Manager to the network before you restart system.

Related Topic
Service Interface Settings

Service Interface Settings

Configure the service interface settings on the Service Interface tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Network Types</td>
<td>Choose the type of network on which the RealPresence Resource Manager resides:</td>
</tr>
<tr>
<td></td>
<td>• IPv4 only</td>
</tr>
<tr>
<td></td>
<td>• IPv4 and IPv6</td>
</tr>
<tr>
<td></td>
<td>• IPv6 only</td>
</tr>
<tr>
<td></td>
<td>If you’re using security certificates, you must request a new certificate if you change these settings.</td>
</tr>
<tr>
<td>System Name</td>
<td>The NetBIOS name (ASCII only) of the RealPresence Resource Manager system server. Must be between 6 and 16 characters long; dashes and underscores are valid characters.</td>
</tr>
<tr>
<td></td>
<td>If you’re using security certificates, you must request a new certificate if you change these settings.</td>
</tr>
<tr>
<td>DSCP Marker</td>
<td>Enables the administrator to configure the Quality of Service level of the RealPresence Resource Manager. Set the level between 0 - 63. The higher the number the higher the Quality of Service level.</td>
</tr>
</tbody>
</table>
Virtualization Settings

If you’re running a RealPresence Resource Manager system, Virtual Edition, you must configure your RealPresence Resource Manager system to match the capacity of your virtual environment. For additional system capability information, see the Release Notes.

Edit Virtualization Settings

For maximum performance, set the system capability of your virtual edition to match the supported number of endpoints. See the RealPresence Resource Manager Release Notes for the supported number of endpoints.

To configure your Virtualization settings:

1. Navigate to Admin > Server Settings > Virtualization Settings.
2. In the System Capability field, enter the number of endpoints that matches your hardware configuration.
3. Click Update.
**Time Settings**

You can configure your system time manually or set it up to synchronize with an external NTP server. If you use an NTP server, be sure to use the same NTP server that is used by your other video conference systems. This will ensure continuity, accurate scheduling, and accurate reports for all systems.

**Edit System Time Settings**

You can update your time settings manually or point your system to an external NTP server. Make sure that 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*.

**To edit the system time settings:**

1. Go to *Admin > Server Settings > System Time*.
2. Configure the system time settings, as necessary.
3. Click *Update*.

**Related Topic**

*System Time Settings*

**System Time Settings**

Configure the system time settings.

<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 RealPresence 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 Synchronization</td>
<td>Select this option to synchronize the RealPresence Resource Manager system date and time with an external NTP server.</td>
</tr>
<tr>
<td>IP address or DNS resolved name</td>
<td>The IP address or fully qualified domain name (ASCII only) of the NTP server. If needed, enter multiple servers separated by a space.</td>
</tr>
</tbody>
</table>

**User Data Collection**

To continually improve the product, it’s important to know how you use the RealPresence Resource Manager system. By collecting this data, Polycom can identify both the system level utilization and the combination and usage of RealPresence Resource Manager features. This usage data will inform Polycom which features are important and are actually used on your system. Polycom will use this information to help guide future development and testing to concentrate on the areas of RealPresence Resource Manager that are most heavily used. If you choose not to send this information, Polycom is less aware of which features
are important to you and that are used by you, which may influence future development to go in directions that are less beneficial to you.

Your decision to enable or not enable the sending of this data doesn’t affect the availability of any documented system feature in any way.

The system sends the data once per hour over a secure TLS connection (port 8443) to a Polycom collection point (customerusagedatacollection.polycom.com). There’s no access by any customer or others to view the data received at the collection point. The raw data will be viewable only by Polycom. To avoid any impact to starting and ending calls and conferences, data is never sent between 5 minutes before the hour and 5 minutes after the hour.

The following types of data are reported:

- License information
- Hardware configuration
- System resource usage: CPU, RAM, disk, database
- System configuration: number of servers, clusters
- Feature usage: Enterprise Directory integration, conference, endpoints, network topology, user management, alert management, and license management.
- Number of users, endpoints, sites, and MCUs.
- Security settings

When this information is reported, a customer’s user and environment identifying information (such as internal IP addresses, and FQDNs, names of users, devices, and external systems) is made anonymous before being sent from the system. System serial numbers and license information are sent without anonymization and may be used to help improve customer experiences. In total, less than 100KB of data per hour is collected and sent.

Enable or Disable User Data Collection

You can enable or disable this feature at any time.

To enable or disable user data collection:

1. Go to Admin > Server Settings > Licenses.
2. Select or clear the Automatically send usage data check box.

View the Collected Usage Data

The system records data that has been sent and collected in the system logs.

To see the collected data:

1. Log in to the RealPresence Resource Manager system as an Administrator.
2. Download the system logs.
3 On the PC where the logs have been downloaded, use an archiving or zipping tool to extract the file analytics.json.
   Analytics.json is a text file containing the hourly data reported most recently before the time when the system logs were created.
4 View the analytics.json file with Notepad or another common text editing tool.
Integrating with an Enterprise Directory

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 log in to the RealPresence Desktop system, RealPresence Mobile, or CMA Desktop system. This happens without the user having to enter their credentials, creating 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.
- Enables 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.

Enterprise Directory Supported Configurations

There are many possible configurations available within Microsoft Active Directory, some of which aren’t fully supported by the RealPresence Resource Manager system. These topics describes the implications of different Microsoft Active Directory configurations for integrating with the RealPresence Resource Manager system.

Single Forest Support

Microsoft Active Directory may be set up in either a single-forest or multiforest configuration. However, the RealPresence Resource Manager system requires that user accounts reside in a single forest.

Multiple Domains within a Single Forest

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 (for example: polycom.com and na.polycom.com would be in the same tree, while polycom.com and resouceManagerDevelopment.net would be separate trees, if they were in the same forest). The RealPresence Resource Manager system will integrate to all domains in a multitree forest.
You can either integrate to all domains of a multidomain forest configuration or restrict to a single domain tree in a multidomain forest through the use of LDAP Search base DN criteria.

**Universal Group Support**

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.

**Read-only Enterprise Directory 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 can’t 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’s important to avoid duplication of account data. For example, if your Active Directory has a user named John Doe with a user name 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 won’t be able to log in to a dynamically managed endpoint.

The RealPresence Resource Manager system accesses the enterprise directory in a read-only mode. It doesn’t 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’s 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 don’t 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.
Integrating with an Enterprise Directory

- 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’s 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.

**Preparing to Use Active Directory**

To take full advantage of the RealPresence Resource Manager system, the enterprise Microsoft Active Directory must meet some requirements.

The Active Directory must:

- Have the 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. Polycom recommends an account with an 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 as follows:

● 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.

**LDAP Searches**

If the RealPresence Resource Manager system is integrated with an Active Directory, the RealPresence Resource Manager 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 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
Integrating with an Enterprise Directory

- Telephonenumber
- Cn
- Samaccountname
- Memberof
- Displayname
- Objectclass
- Title
- localityName
- department

**Related Topic**

**Searching in a List**

**Using the Base DN to Manage Enterprise Directory Searches**

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 is the starting point in the Active Directory hierarchy at which your search will begin.

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’ve established a working connection with your Active Directory, then you enter a **Base DN**.

For complete documentation on using Base DNs, see the documentation for Microsoft Active Directory.

**Examples of Base DN Filter Expressions**

The following table illustrates some basic examples of Base DN filter expressions.

<table>
<thead>
<tr>
<th>Search base DN 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 **Base DN** field. They include:
The special characters that aren’t allowed in the **Base DN** field. The special escape character (backslash, \) are:

<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>”</td>
</tr>
</tbody>
</table>

The special characters that aren’t allowed in the **Base DN** field. The special escape character (backslash, \) are:

<table>
<thead>
<tr>
<th>Character</th>
<th>Character Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>“ \ ”</td>
<td>Backslash</td>
</tr>
<tr>
<td>“ = ”</td>
<td>Equal</td>
</tr>
<tr>
<td>“ : ”</td>
<td>Comma</td>
</tr>
<tr>
<td>“ # ”</td>
<td>Pound</td>
</tr>
<tr>
<td>“ + ”</td>
<td>Plus</td>
</tr>
<tr>
<td>“ ; ”</td>
<td>Semicolon</td>
</tr>
<tr>
<td>“ &lt; ”</td>
<td>Less than</td>
</tr>
<tr>
<td>“ &gt; ”</td>
<td>Greater than</td>
</tr>
</tbody>
</table>

Therefore, to use these characters as part of a name, they must be preceded in the **Base DN** field by a backslash. For example, the base DN of an ou named "tom,ann,bob" in the "myteam.example.com" domain must be entered as:

\ou=tom\,ann\,bob\ dc=my team,dc=example,dc=com

Or the base DN of an ou named "#+,=<\>\ " in the "mydomain.example.com" domain must be entered as

\ou=\#+\,=\,<\>\,\ dc=mydomain,dc=example,dc=com
Integrating with an Enterprise Directory

Note that this applies only to attribute values, not the ou= or dc= structure.

Examples of Base DN 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 base DN 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>Excludes 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 don’t use medial searches when implementing exclusion filters.

Examples of Advanced Base DN Exclusion Filters

The following table illustrates some more advanced examples of exclusion filter expressions.

<table>
<thead>
<tr>
<th>Search base DN 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>
</tbody>
</table>

Notes:
- The expression should be in continuous line with no carriage returns or extra spaces (not possible in this document’s format).
- By excluding an entity, we implicitly mean to include all other entities. Conversely, by including an entity, we’re 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.

<table>
<thead>
<tr>
<th>Search base DN expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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

When the RealPresence Resource Manager system must be integrated with an Active Directory server and trusted by Active Directory, users with dynamically managed endpoints can securely log in to their endpoint without typing in their network credentials.

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 in to the RealPresence Resource Manager system, it authenticates the user by connecting to the domain controller that it’s 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 in to the workstation.

Because the RealPresence Resource Manager system uses NTLMv2, the password isn’t 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 isn’t joined to the domain. Other computers on the network can’t browse its file system and it cannot be managed remotely by existing IT mechanisms such as SMS.
- The RealPresence Resource Manager system doesn’t 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 doesn’t 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.

Managing Directories

Integrating the RealPresence Resource Manager with an enterprise directory server enables you to manage the directories from the RealPresence Resource Manager system.

Integrating with Enterprise Directory Server

Enabling the Integrate with Enterprise Directory Server option enables RealPresence Resource Manager system users who are included in the Active Directory to log in to the RealPresence Resource Manager system interface using their network credentials.
Enabling the **Integrate with Enterprise Directory Server** option also enables 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.

**Create the 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.

You need to create a service account in Active Directory for the RealPresence Resource Manager system to use.

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 log on name** fields, type `resourcemangerservice` 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

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 doesn’t have to match the host name of your RealPresence Resource Manager system server.

You need to create a computer account in Active Directory for the RealPresence Resource Manager system.

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. Log in 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 polycomrm$ p@ssw0rd

   Performing the net user command on any machine other than a domain controller won’t 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

Enabling the Integrate with Enterprise Directory Server option enables RealPresence Resource Manager system users who are included in the Active Directory to log in to the RealPresence Resource Manager system interface using their network credentials.
Enabling the Integrate with Enterprise Directory Server option also enables 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.

**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 the enterprise directory integration settings.
5. Click Update.

**Related Topic**

Enterprise Directory Integration Settings

**Enterprise Directory Integration Settings**

Configure the enterprise directory integration 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 in the Create the RealPresence Resource Manager System Service Account section. 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's 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>
<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: • Plain—No security on the connection • LDAPS—The connection is secured over outbound port 3269 using LDAPS 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.</td>
</tr>
</tbody>
</table>
Integrating with an Enterprise Directory

Polycom, Inc. 62

Allow Delegated Authentication to Enterprise Directory Server

The RealPresence Resource Manager system Use Single Sign on (Integrated Windows Authentication) option, enables endpoint users who are included in the enterprise directory to securely log in to their dynamically managed endpoint without typing in credentials.

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. Do one of the following:
   - in the Domain controller name section enable Auto-discover for the system to automatically discover the closest logical domain controller and enterprise directory servers.
   - To use the auto-discover option, the network DNS server must contain the DNS SRV records for these servers.
4. 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).

   If you use an unstable Active Directory Resource Pool, Polycom recommends that to specify the fully qualified hostname of the domain controller to avoid issues.

5. Enter the Username (domain\<computer name>) and Password and click Update.

Give Enterprise Users Default Scheduler Role

By default when local users are added to the RealPresence Resource Manager system, they’re assigned the Scheduler role. By default, when you integrate a RealPresence Resource Manager system to an Active Directory, enterprise users aren’t 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use LDAP Filter</td>
<td>Specifies which user accounts to include (an underlying, non-editable filter excludes all non-user objects in the directory). The default expression includes all users that don’t have a status of disabled in the directory.</td>
</tr>
<tr>
<td>Enterprise Directory Search Base DN</td>
<td>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 Using the Base DN to Manage Enterprise Directory Searches.</td>
</tr>
</tbody>
</table>
To give enterprise users default Scheduler role:

1. Go to Admin > Directories > Enterprise Directory.
2. Select the Associate Enterprise users with basic scheduler role by default check box.
3. Click Update.

Change the Message for Enterprise Users without a Role

You can customize the message enterprise users see when they attempt to log in but don’t have a user role assigned.

To change the message enterprise users without a role, see when they try to log in:

1. Go to Admin > Directories > Enterprise Directory.
2. Edit the Message to be displayed to unauthorized users.
   - For example, enter a message such as “Your user name and password are valid, but you have no permissions on this system. Contact your IT department for more information.”
3. Click Update.

Select SMB Version

You can select the version of the SMB protocol to connect with the enterprise domain controller.

To select the SMB version:

1. Go to Admin > Directories > Enterprise Directory.
2. Select a SMB version to use from Select SMB to connect with the Domain Controller.
3. 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. You can use the Directory Setup options to affect which devices and users appear in the endpoint directory.

Typically, endpoints that don’t use the RealPresence Resource Manager as register for the Polycom GDS and are listed in the RealPresence Resource Manager system Global Address Book. The Global Address Book enables 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.
Global Address Book Tips

- The RealPresence Resource Manager system Global Address Book lists endpoints. Endpoints may or may not have users or rooms associated with them. On an endpoint, the Global Address Book doesn't list users unless they have endpoints associated with them.
- If your company has more than 100 endpoints, don't limit the Global Address Book on the endpoint side or the endpoint user won't have access to all Global Address Book entries.
- The RealPresence Resource Manager system Global Address Book does not support unicode data.
- Nondynamically managed endpoints are listed in the Global Address book regardless of if they’re associated with an owner.
- For Desktop 3.2 endpoints, the device model is also shown in the directory listing.

Including or Excluding Dynamically Managed Endpoints in the Global Address Book

By default the RealPresence Resource Manager system includes all dynamically managed endpoints in the Global Address Book.

The Include dynamically managed devices in the Global Address Book option changes the Global Address Book so that it also includes all dynamically managed endpoints. In this case, the Global Address Book limit is increased to 5000 entries. (Dynamically managed endpoints are always included in the enterprise LDAP directory.)

Include Enterprise Users

You can include enterprise users in the RealPresence Resource Manager system Global Address Book.

To include enterprise users in the RealPresence Resource Manager system Global Address Book:

2. In the Directory page, select Include dynamically managed devices in the Global Address Book.
3. Click Update.

Remove Enterprise Users

You can remove enterprise users from the RealPresence Resource Manager system Global Address Book.

To remove enterprise users from the RealPresence Resource Manager system Global Address Book:

2. In the Directory page, clear Include dynamically managed devices in the Global Address Book.
3. Click Update.
**Including or Excluding 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. The **Show Guest Book entries in the Directory** option is also selected by default.

**Include Guest Book**

You can include Guest Book entries in the endpoint directory.

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**.

**Remove Guest Book**

You can remove Guest Book entries from the endpoint 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**.

**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, select the **Allow endpoint directories for local users to include enterprise directory user information** check box.
3. Click **Update**.

**Supporting 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.
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, select 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 setup, 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 > Scheduled Management > Provisioning Profiles.
2. Click .
3. In the Add Profile dialog, select LifeSize in the Endpoint Type drop-down list, enter a name for the profile, and click OK.
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 Profiles.
5. For Directory support, select the Directory > LDAP.
6. On the Directory > LDAP page:
   a. Select 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’ve 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.

Related Topic

Endpoint Fields for Scheduled Provisioning Profiles
Allow Mid-String Searches for Local Users

By default, you can only search for local users by the initial letter(s) or number(s) of the user ID. If you enable midstring searches for local users, you can search by any character in the user ID.

For example, if you type "oo", you'll see the following results:

TeslaRoom
TurinRoom
EinsteinRoom

To allow for midstring searches for local users:

2. Select the Allow mid-string search for local user/room/guest and legacy endpoint check box.
3. Click Update.
License Management

The RealPresence Resource Manager system manages both its own licenses and licenses of other Polycom products and features.
License Management

RealPresence Resource Manager manages the licenses for both features and devices.

System Licensing

The device management capacity for a RealPresence Resource Manager system with the scales from 100 to 50,000 devices. The minimum capacity of a RealPresence Resource Manager system is of 100 client access licenses. Additional licensing is offered in 100, 500, and 1000 license pack sizes.

When applied to the system, an expansion license pack augments the device license count.

Device licenses are consumed based on a 1:1 basis for any managed device (endpoints, MCU, GW—including personal endpoints, and more). The devices can be added to the system by any means, including the user interface, registration for management services, or registration for Global Address Book services. This includes the following device types:

- Endpoints synchronized from an integrated RealPresence DMA system
- Any managed video endpoint, both dynamic and scheduled (RealPresence Immersive Studio systems and other Polycom ITP systems consume three device licenses, one for each codec.).
- Any managed audio endpoint
- A RealPresence Access Director system
- A RealPresence DMA system
- A RealPresence Collaboration Server
- A Cisco Unified Communications Manager

Device licenses are consumed by managed devices, not by users. You may add any number of local or enterprise users to the RealPresence Resource Manager system.

The RealPresence Resource Manager system has the following feature licenses:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Tenancy</td>
<td>Enables you to use the areas feature to partition collections of resources.</td>
</tr>
<tr>
<td>Video Endpoint License Management</td>
<td>Determines the number of endpoints that you can manage.</td>
</tr>
<tr>
<td></td>
<td>If you are a RealPresence One customer, this license is disabled and governed by your RealPresence One subscription.</td>
</tr>
<tr>
<td></td>
<td>Video endpoints license can also be used to manage audio endpoints.</td>
</tr>
</tbody>
</table>
Licensing for RealPresence software clients is included with the RealPresence Resource Manager system. RealPresence software clients include Polycom CMA Desktop, RealPresence Desktop and RealPresence Mobile clients.

When a software client is provisioned by the RealPresence 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 time (days) of inactivity.

Dynamically managed Polycom endpoints (both hardware and software endpoints) are automatically deleted from the system after 6 months of inactivity, which is independent of the license reclamation for Polycom software endpoints.

Non-dynamically managed endpoints are never automatically released. To release a license from a registered endpoint, an administrator must manually delete the device from the system.

Reclaim Software Client Licenses

**Video Endpoint and Phones License Control (Non-Polycom RealPresence Clariti)**

For a-la-carte and non-Polycom RealPresence Clariti appliance versions, video endpoint license and phones licenses are separately controlled. Video endpoint license can be used to manage audio endpoints. Audio endpoints license cannot be used to manage video endpoints.

Under a-la-carte mode, you can active phone and endpoint license on your license server on Polycom License Center. On the RealPresence Resource Manager GUI, you can view the audio and video endpoint license allocation on the License > Allocation page.

On the Dashboard, you can view the video and audio license usage information from the Video Endpoint Licenses and Audio Endpoint Licenses panes.

You can set video and audio license alert level on the Alert > Alert Level Settings page.

Dashboard Panes

Set Endpoint Alert Level Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Endpoint License Management</td>
<td>Determines the number of audio endpoints that you can manage. Audio endpoints license cannot be used to manage video endpoints.</td>
</tr>
<tr>
<td>Service Provider API</td>
<td>Enables you to access RealPresence Resource Manager functionality via the API</td>
</tr>
<tr>
<td>Redundant system licenses (primary and redundant licenses)</td>
<td>Enables you to set up redundant systems.</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>Enables encryption for chat and presence (XMPP) service.</td>
</tr>
</tbody>
</table>
Trial Licenses for Appliance Editions

Appliance editions come with a trial license file that is valid for 60 days after activating your system. The trial license also enables the optional Polycom RealPresence DMA system integration, multi-tenancy, and Service Provider API capabilities for 60 days.

With your system order for an appliance edition, you'll receive one or more License Certificates. You must activate the License Certificate to receive a license file, which you then upload to the RealPresence Resource Manager system. When you update this license file, it overwrites the trial license file.

Adding System Licenses for an Appliance Edition for Non-Polycom RealPresence Clarity

If you aren't a RealPresence Clariti customer, to add licenses to your RealPresence Resource Manager system, Appliance Edition, you need to request a software license file and then update it.

Request a Software License File

If you aren’t a RealPresence Clariti customer and have an appliance edition, you need to request a license file from the Polycom technical support website.

To request a software license file:

1. In a separate browser page or tab, log in to the RealPresence Resource Manager system server as an administrator.
2. Go to Admin > Server Settings > Licenses and record the RealPresence 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’ll need to load both license files onto your primary server, see System Redundancy.
11. In the Key Code field, click here to download to retrieve and save your license files.

System Redundancy
Update the License File

You can update the license file for your appliance edition system at any time. For example, if you purchase more device licenses or add features. After you update a license file, you must log out and relogin to the system to see newly licensed features.

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, click Update.
6. You must log out of the system and log back in to view any new licensed features such as multi-tenancy or RealPresence DMA integration features.

View Current Licensing

You can view the current licensing status and information.

To view current system licensing for a Virtual Edition:
1. Go to Admin > Server Settings > Licenses.
   The Licenses page displays the following license related information when you have a virtual edition.
   - System licensing is handled by the license server. Please check the license server for license details.
     - License Server Address
     - License Server Port
     - Last time connecting to the license server successfully
     - Last time attempting to connect to license server
   - End User License Agreement
     - Status
     - Automatically send usage data
   - Reclaim Inactive RealPresence Software Client Licenses
   The Licenses page displays the following information when you have an appliance edition.
   - Software Version
   - Serial Number
   - Supported Versions
   - Server Type
   - Licenses Status
   - Site Duration
   - End User License Agreement
License Management

♦ Status
♦ Automatically send usage data
  ➢ Reclaim Inactive RealPresence Software Client Licenses

Reclaim Software Client Licenses

Polycom RealPresence Desktop, RealPresence Mobile and CMA Desktop clients don’t release licenses automatically when they aren’t 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. The threshold time limit is measured in days.

However, unlicensed software endpoints are kept in the system until the total number of soft endpoints (licensed and unlicensed) exceeds 90 percent of four times the number of allowed licenses. This allows software endpoints to remain in the RealPresence Resource Manager system, retain their dial string reservations, and to be scheduled into conferences.

For example, if you have purchased a license for 500 endpoints, you can keep up to 90 percent of four times 500, or 1800 total endpoints (software and hardware) in the system at one time. While only 500 of those endpoints will be licensed, unlicensed software endpoints will remain associated with user dial strings so that the user can still be scheduled into conferences and remains in the system if the user wants to use the software endpoint at any time.

The RealPresence Resource Manager system automatically deletes unlicensed software endpoints when the 90 percent of four times the number of allowed licenses is reached. It started deleting software endpoints based on number of days of inactivity, starting with the most number of days.

To set the threshold for reclaiming inactive 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. The threshold time limit is measured in days.
   To reclaim licenses more quickly, lower the threshold. Set the threshold to 0 days, to stop reclaiming licenses.
3. Click Update.

Licensing RealPresence Platform Components

Polycom RealPresence Resource Manager is available as part of Polycom RealPresence Clariti, a Polycom collaboration infrastructure offer that features simplified concurrent user licensing and add-on options. RealPresence Clariti customers should consult with their Polycom representative to ensure that they have the correct licensing information before upgrading.

If you’re a RealPresence Clariti customer, you must use the RealPresence Resource Manager system to license your product. RealPresence Resource Manager to manage licenses for the following products that support RealPresence Clariti:

- Polycom RealPresence DMA, Virtual, and Appliance Editions
- Polycom RealPresence Access Director, Virtual, and Appliance Editions
License Management

- Polycom RealPresence Collaboration Server, Virtual Editions
- Polycom RealPresence Media Suite, Virtual and Appliance Editions
- Polycom RealPresence Web Suite Experience Portal
- Polycom RealPresence Web Suite Services Portal

If you have a RealPresence Clariti solution subscription, you can view or download license usage data for up to 180 days.

**Managing License for RealPresence Web Suite**

You can choose to manage your RealPresence Web Suite instances with RealPresence Resource Manager.

If you have RealPresence Web Suite included in your system, you can run those instances in either way:
- Install the instances outside of your RealPresence Resource Manager system and manage licenses using their existing license management process.
- Add the instances to your RealPresence Resource Manager system to manage them.

See *Polycom RealPresence Web Suite Administrator Guide* for instructions on how to associate the RealPresence Web Suite Services and Experience Portals and set up licensing for those two servers within RealPresence Resource Manager.

**Managing License for Polycom® ContentConnect™ Solution Server**

License features for a Polycom ContentConnect solution server (for example, Base License for ContentConnect software and High Availability) aren’t displayed on the License Management page as uncounted licenses when you select the License > Allocation. However, you can point the ContentConnect license server to RealPresence Resource Manager to retrieve uncounted licenses.

**Managing License for a RealPresence DMA Supercluster**

RealPresence Resource Manager manages licenses for RealPresence DMA systems in a supercluster separately. If you have a RealPresence DMA supercluster, you must add all the RealPresence DMA systems in a supercluster to the RealPresence Resource Manager system. In the RealPresence Resource Manager system, you can allocate licenses for the RealPresence DMA systems in a supercluster separately.

**Enable Licensing for a Network Device**

To use RealPresence Resource Manager as license server, you must enable licensing when you add the instance of the product that you want to license.
To enable licensing:

1. Go to Network Device > Instances.
2. Select an instance of interest and click Edit.
3. Select a device type that you want to add.
4. For the device types that can be licensed, you’ll see the License Configuration tab. Select the Enable Polycom License Server Licensing check box to enable license control.
5. Click OK to save the changes.

Online and Offline Mode

Licenses for RealPresence Resource Manager system components can be managed in online or offline mode. If the data center where the RealPresence Resource Manager system is located has connectivity to the Internet, you must use online mode to manage licenses. If the data center doesn’t have Internet connectivity, you can manage the RealPresence Platform components in offline mode.

Allocate Licenses for Polycom RealPresence Platform Components

You can allocate licenses for individual components of your RealPresence Platform deployment after you set up the license server and activate RealPresence Platform licenses within RealPresence Resource Manager.

All license allocations for individual product are managed through the RealPresence Resource Manager License menu.

A system component must be online within the RealPresence Resource Manager system, and the system component time must be synchronized with RealPresence Resource Manager before licenses can be successfully allocated to the component. If a system component is offline during license recovery, its allocated licenses will be cleared.

In addition, the credentials for the system user configured for the component within RealPresence Resource Manager must match the credentials for the system user as configured within the component system.

If a license allocation fails for a newly added Polycom RealPresence virtual instance, verify that:

- The inbound ports required for license-related communications (3333 and 9333) are open on RealPresence Resource Manager.
- The IP address configured in RealPresence Resource Manager is the correct address for the instance. A license allocation will fail if the IP address selected for a virtual instance does not match the instance type to which features are allocated.

If you want to reinstall the old Polycom platform components or servers that have already been licensed, you must delete the old instances from RealPresence Resource Manager before reinstallation. After the reinstallation, you must redeploy and reallocate licenses for the instances.

For a redundant system, servers switch may cause off line network components license allocation failure. In this case, you need to make the components online and reallocate licenses for them.
To allocate licenses to a RealPresence Platform component:

1. Go to License > Allocation and do one of the following:
   - Select Allocate By: Type to select a product type and see the instances of that type managed by RealPresence Resource Manager. Then select a product instance to see a list of applicable licenses and allocate licenses to that specific instance.
   - Select Allocate By: Feature to see a list of all the activated licenses. Then select a license feature to see the product instances to which that license is applicable and allocate the license feature to specific instances.
     For count-based license features (such as max calls), note the number available and set the allocation input field to the number to allocate to the current instance.

2. Click Save.

3. Repeat step 1 and step 2 to allocate additional license features to the selected product instance or allocate the selected license feature to additional product instances.

4. After allocating licenses, go to the license settings page within each product instance you licensed to verify that the new licenses are available to the product. See the product documentation for instructions on how to view licensing information.

   For RealPresence Collaboration Server and RealPresence Access Director products, license allocation changes take effect only after those systems have been rebooted.

**Reset Allocated Licenses**

You can take the allocated licenses back per instance and re-allocate the licenses for the Polycom RealPresence Platform components.

To reset allocated licenses:

1. Go to License > Allocation.
2. Go to the feature for which you want to re-allocate the license.
3. Click Reset.

**Clean Unused Licenses**

You can clean all the allocated, but unused licenses that do not take effect for the Polycom RealPresence Platform components. Use this function only when you run into problems with license allocation.

To clean unused licenses:

1. Go to License > Allocation.
2. Click Clean.
Update the Licenses of Polycom RealPresence Platform Components

When you buy additional features or capacity for your RealPresence Platform components, you must allocate the newly available licenses to your RealPresence Resource Manager license server and activate them within RealPresence Resource Manager. For counted licenses, you can now allocate them to one or more appropriate system components.

To allocate and activate newly available licenses:

1. In the RealPresence Resource Manager management interface, go to License > Setup and copy the System Identifier number listed on the page.

2. In a different browser window, log in to the Polycom Licensing Center using the URL and credentials sent to you.
   
   See the Polycom RealPresence Resource Manager Getting Started Guide for information about using the Polycom Licensing Center.

3. Click Search Servers, paste the copied system identifier number into the License Server ID field, and click Filter.
   
   Your RealPresence Resource Manager license server appears in the list below.

4. Click the license server ID in the list below.
   
   The View Server page displays license information for this RealPresence Resource Manager license server.

5. Click Map Add-Ons.
   
   The Map Add-Ons page displays a table of license information for your organization, showing usage and availability.

6. Find the license add-ons you want to allocate and verify that Available Units in Line Item are not zero.

7. In the Qty to Add field of the add-ons you want to allocate, enter the number of units to allocate to this RealPresence Resource Manager instance and click Map Add-Ons.
   
   The View Server page returns, displaying a list of the server’s licenses. The status for newly allocated licenses is License not generated. The licenses must be generated (activated within your RealPresence Resource Manager system).

8. If you allocated too many license add-on units to this RealPresence Resource Manager instance and want to remove some, click Remove Add-Ons.
   
   The Remove Add-Ons page lists the license add-ons available on this instance.

9. In the Quantity to Remove field of the add-ons you want to change, enter the number of units to remove and click Remove Add-Ons.
   
   The View Server page returns, displaying a list of the server’s licenses. The status for licenses with newly removed units is Copies decreasing. The removed licenses must be deactivated within your RealPresence Resource Manager system.
10 If your RealPresence Resource Manager instance doesn’t have access to the Internet, click **Download Capability Response** to download a local copy of the license file. Note the location of the license file when you download it to your local computer.

If your RealPresence Resource Manager system has access to the Internet, you must use the online method to license the system and its components. The offline method for managing licenses isn’t an option when Internet access is available.

11 Return to the **RealPresence Resource Manager License Setup** page, and do one of the following:

- Click **Online** if your virtual environment has access to the Internet and can use the online method for managing licenses.
- Click **Offline** if your virtual environment doesn’t have access to the Internet. Prompts guide you through the offline update process using the license file you previously downloaded from the Polycom Licensing Center.

12 Click **Update** to complete the license activation process.

   The licenses should be activated within a few seconds to a minute. You may need to refresh the browser window.

**Related Topic**

*Allocate Licenses for Polycom RealPresence Platform Components.*
System Setup Overview

Based on your system design and installation, you may need to complete some configuration tasks to complete your implementation of a Polycom RealPresence Resource Manager system after First Time Setup.

Setting Up Network Device Management

You need to set up your RealPresence Resource Manager system to monitor your video conferencing infrastructure as well as license any included Polycom infrastructure products.

- Add instance to the system for service integration, licensing, and monitoring. See Managing Instances for details.
- Configure service groups settings. See Managing Service Groups for details.

Configuring Conferencing

You need to configure the RealPresence Resource Manager system for conference monitoring and scheduling.

Related Topic

Setting up Site Topology
Setting up Conference Templates
Set Up Directory Services

Setting 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.

Related Topic

Setting Up Site Topology
Setting 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. See Direct Conference Templates for more information.

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:

1. For endpoints under scheduled management, set up and register endpoints.
   a. Set the Global Directory Server (GDS) to point to the RealPresence Resource Manager system IP address or DNS name. Polycom recommends using the IP address to prevent data inconsistencies.
   b. Register the endpoints to the Polycom RealPresence 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 RealPresence 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.

2. For endpoints under scheduled management, 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, User ID, Password, and Email Address) is directly pulled from the directory and cannot be changed. However, you must still associate enterprise users with endpoints.

3. Set up groups, add members, and associate them with provisioning profiles. For more information,

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.

Managing Meeting Rooms

Configuring the Connection to an External Enterprise Directory

Connecting to an enterprise directory enables users to enter their network usernames and passwords to log into RealPresence Resource Manager system and dynamically managed endpoints. It also enables users to access the enterprise directory when selecting conference participants.
Your RealPresence Resource Manager system must be connected to an enterprise directory system of Microsoft Active Directory in order to dynamically manage the Polycom endpoints. Dynamic endpoint management enables rule-based provisioning profiles and dynamic software updates.

You can configure your RealPresence Resource Manager system to use an enterprise directory at any time.

Related Topic
Integrating with an Enterprise Directory

Setting Up Endpoint Management

You can manage endpoints with the RealPresence Resource Manager system by either scheduled management or dynamic management.

Scheduled Management of Endpoints (Polycom and Third-Party)

Scheduled management enables you to push software updates and provisioning profiles to endpoints at intervals that you define.

Scheduled management uses server-to-client communication over HTTP. This management technique is appropriate for corporate networks where both the RealPresence Resource Manager and all endpoints are behind the same firewall.

Related Topic
Scheduled Endpoint Management

Dynamic Management of Endpoints (Polycom Only)

Dynamic management enables the endpoint to poll the RealPresence Resource Manager system automatically to get dynamic provisioning profiles (configuration settings) and software updates on a regular basis.

Dynamic management is client-to-server over HTTPS which makes it more secure and firewall-friendly.

Dynamic management is:

- available only for Polycom video endpoints.
- optional when your system is integrated with an enterprise directory.
- recommended when Polycom endpoints are able to automatically discover the RealPresence Resource Manager. This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager.

In dynamic management mode, when an endpoint starts up at designated intervals thereafter, it automatically polls the RealPresence Resource Manager system for a newer software update package or provisioning profile. If 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.
Setting up Phones Management

The RealPresence Resource Manager system can be used as a central provisioning server for supported phones. When a phone is provisioned, it polls the RealPresence Resource Manager system for configuration profile settings and software updates at intervals that you define.

Securing the 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.

Configuring Redundancy (Optional)

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

A redundant RealPresence Resource Manager system configuration requires the installation of two RealPresence Resource Manager system servers. During First Time Setup, you are instructed to assign these two servers physical IP addresses.

Distributing Polycom Applications

The RealPresence Resource Manager system enables you to download several Polycom applications for use in specific environments. This includes two desktop video applications.
Network Device Management

You can use RealPresence Resource Manager to manage network devices, instances, and service groups.
Understanding Network Device Management

The Polycom RealPresence Resource Manager system acts as network device management console for systems within your video infrastructure environment.

Network devices include any infrastructure device that the RealPresence Resource Manager system manages, licenses, or is aware of.

You can add network devices to the RealPresence Resource Manager system for monitoring, licensing, as well as service integration, depending on the product.

You can access individual products directly from the RealPresence Resource Manager system device management console after you have added them to the system. In addition, you can manage the time, SNMP, and Active Directory settings for all network devices via a service group.

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 Device Management

You can add network devices to the RealPresence Resource Manager system for monitoring, licensing, as well as service integration, depending on the product.

Service Integration

When you integrate a product's services with the RealPresence Resource Manager system, it uses those services for conference scheduling and management as well as endpoint provisioning.

Monitoring

When you add an instance of a network device to the RealPresence Resource Manager, it can monitor the system. When the RealPresence Resource Manager monitors a system, it tracks the health of the system and you can also view whether or not the network device is available or offline.

Service Group Administration

When you add network devices to the RealPresence Resource Manager system, they are added to the default service group. A service group is a group of network devices that can be monitored together and inherit some server settings from the service group settings. You can manage the following settings through service group settings: password settings, time settings, SNMP settings, and Active Directory integration settings.
When you configure settings for a service group, the settings are inherited by supported Polycom network devices within the group.

**Licensing**

The RealPresence Resource Manager provides the licensing interface between Polycom products and the Polycom Licensing Server. Most RealPresence Clariti products can be licensed via the Polycom Licensing Server.

**Supported Network Devices**

The RealPresence Resource Manager system supports these network device types:

<table>
<thead>
<tr>
<th>Network Device</th>
<th>Service Integration</th>
<th>SNMP Monitoring</th>
<th>API Monitoring</th>
<th>Licensing</th>
<th>Service Group Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealPresence Collaboration Server</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>(Virtual Edition Only)</td>
</tr>
<tr>
<td>Polycom MGC</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>RealPresence DMA system</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Non-high availability systems only</td>
</tr>
<tr>
<td>RealPresence Access Director</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Polycom VBP</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Acme SBC</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>RealPresence Web Suite</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>RealPresence Media Suite</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>

**Network Device Types**

You can filter the network device on **Network Device > Instances** by device types.

- **VBP** (Video Border Proxy systems)—Displays the list of Polycom VBP systems registered to the RealPresence Resource Manager system.
- **ACME SBC** (Session Border Control systems)—Displays the list of SBC systems registered to the RealPresence Resource Manager system.
- **RealPresence Collaboration Server/MGC** (MCU)—Displays the list of Polycom MCUs registered to the RealPresence Resource Manager system.
- **RealPresence DMA**—Displays the RealPresence DMA system registered to the RealPresence Resource Manager system.

- **RealPresence Access Director**—Displays the list of RealPresence Access Director systems registered to the RealPresence Resource Manager system.

- **RealPresence Web Suite Services/Experience Portal**—Displays the list of RealPresence Web Suite Service Portals and Experience Portals registered to the RealPresence Resource Manager system.

- **Cisco Unified Communications Manager**—Displays the information related to the Cisco Unified Communication Manager, if integrated with the RealPresence Resource Manager system.

- **RealPresence Media Suite**—Displays the list of RealPresence Media Suite licensed by the RealPresence Resource Manager system.
Managing Instances

An instance is a Polycom video infrastructure component (network device) that runs on a virtual machine or a hardware appliance. When you add a component to the RealPresence Resource Manager system, you can choose to use RealPresence Resource Manager to monitor the alarms, manage licensing for the components, or/and integrate this component with the RealPresence Resource Manager system. You can add both virtual and appliance edition products as instances in RealPresence Resource Manager.

If you work under vCenter environment, see Appendix A: Working in a vCenter Environment on how to manage instances, images, and providers.

Related Topic
Working in a vCenter Environment

View Network Device Instance

By default, all the instances that you have added are displayed on the Instances page.

To view network device instances:

1. Go to Network Device > Instances.
2. Click Filter to filter the instances that you want to display. You can filter instances by Device Type, Device Name, IP Address, or Site.
3. Select an instance that you want to view.
4. Click View Details to display a summary of this instance.

Related Topic
Network Device Details

Network Device Details

The Network Device list has the following fields:
Add an Instance by IP

You can add existing appliance instances and virtual instances by IP address. Before you add an instance, verify that you are using the correct IP address and that the instance is running and accessible from its own user interface.

To add an existing instance by its IP address:

1. Go to Network Device > Instances.
2. Click Add.
3. Select a device type that you want to add.
   
   Based on the selected device type, you may see different fields under the Device Type tab. For most device types, you need to provide **Device Name**, **Version**, **IP Address**, **Admin User**, and **Admin Password**.
   
   The format of **Version** is **X.X.X** and must be all numbers. For example, 6.4.0 is a correct version number but v6.4.0 is incorrect.
4. For the device types that can be integrated, you will see the **Service Integration** tab, select the check box under this tab to enable service integration.
5. For the device types that can be licensed, you will see the **License Configuration** tab, select the **Enable Licensing with the Polycom License Server** check box to enable licensing.
6. Select **IP or FQDN Address** from the **Add By** drop-down list.
7. Click **OK** to add the instance to the RealPresence Resource Manager system.
Managing Instances

**Edit an Instance**

Editing an instance allows you to update its certain parameters.

**To edit an instance:**

1. Go to Network Device > Instances.
2. Select an instance you want to edit.
3. Click Edit 🆕.

**View an Instance**

You can view the summary of an instance name and version.

**To view an instance:**

1. Go to Network Device > Instances.
2. Select an instance you want to view.
3. Click View Details ☑.

**Delete an Instance**

After you delete an instance, all its service integration and license control is deleted.

**To delete an instance:**

1. Go to Network Device > Instances.
2. Select the instance you want to delete.
3. Click Delete ✗.
4. Click OK to confirm the deletion.
Managing Service Groups

A service group is a logical collection of hardware appliances and/or virtual machine instances that are configured to work together. A service group might consist of a RealPresence DMA instance, one or more RealPresence Collaboration Server Systems, RealPresence Web Suite Services and Experience Portals, and others.

The instances in a service group are typically configured to work together to provide video collaboration services to the users of various Polycom audio and video collaboration systems in your organization’s locales. A service group could represent a service provider creating a group that serves a particular enterprise, one campus of an enterprise, a division or geographical locale within a company, or any other group recognized by your organization. With these related instances placed in a logical group, they can be monitored as a unit and measured to determine usage statistics.

With a service group, you can manage and monitor multiple types of instances on a single map and view a graphical representation of their usage.

The service group map allows you to navigate to any Polycom network device within the service group. When you navigate to a network device to manage it, you can view the web interface for that network device in a new tab on your browser.

You can also set service group-level settings such as time settings, SNMP, and Active Directory integration.

Create a Service Group

Create a service group to designate appliance and virtual instances that together provide a distinct service within your organization.

To create a service group:

1. Go to Network Device > Service Groups.
2. Click Add Service Group from the Service Group drop-down list.
3. Enter a Name and Description for the new service group.
4. Click OK to save the new service group.
5. From the Service Group drop-down list, click Edit beside the new service group.
6. Click the Instance tab.
7. In the Available section, select the instance(s) that you want to add to the service group and click the arrow icon to move the list to the Selected section.
8. Click OK.
Edit Service Group Details

You can edit the name and/or description of an existing service group.

To edit a service group:

1. Go to Instance Deployment > Service Groups.
2. Select the Service Group you want to edit from the Service Group drop-down list from the top-right corner.
3. Click Edit besides the service group that you selected.
4. Update the Name and Description fields as necessary.
5. Add or remove instances as necessary.
6. Click OK to confirm the changes.

Delete a Service Group

You can delete the existing service groups that you created.

To delete a service group:

1. Go to Instance Deployment > Service Groups.
2. Select the Service Group you want to delete from the Service Group drop-down list from the top-right corner.
3. Click Delete besides the service group that you selected.
4. Click OK to confirm the delete.

Configuring Common Settings for a Service Group

You can configure common settings for a service group. When you configure settings at the service group level, all Polycom products within the service group inherit those settings from the service group settings.

You can configure time settings, SNMP, and Active Directory integration at the service group level.

Polycom RealPresence Collaboration Server 8.5 does not support the common settings.

Configure Time Settings for a Service Group

To configure the time settings for a service group, you can configure the group to use an NTP server (recommended) or manually set the system time settings for the service group systems.

The common time settings only apply to the following servers in a service group:
To configure time settings for network device service group:

1. Go to Network Device > Service Groups.
2. Select the service group you want to configure from the Service Group drop-down list in the right corner of the screen.
3. Click Time Settings.
   The Time Settings dialog box displays.
4. In the Time Settings dialog, select a time zone from the System Time Zone drop-down list.
5. To use an NTP server:
   a. Select the Use NTP Server radio button.
   b. Add the IP address or host name of the server you want to use.
6. To use the system time:
   a. Select the Use System Time radio button.
   b. Configure the system date and time using the fields provided.
7. Click OK.

Configure SNMP Settings for a Service Group

You can configure which version of SNMP to use as well as set up notification receivers to help you track network device activities.

The SNMP settings only apply to the following servers in a service group:

- Polycom RealPresence Resource Manager
- Polycom RealPresence DMA
- Polycom RealPresence Access Director
- Polycom RealPresence Collaboration Server
- Polycom RealPresence Web Suite

To enable SNMP for a service group:

1. Go to Network Device > Service Groups.
2. Select the service group you want to configure from Service Group drop-down list in the right corner of the screen.
3. Go to SNMP Settings.
4. Select the Enable SNMP monitoring check box.
5. In the Agent Settings area, configure the settings.
6. Click Update.
7 In the **Notifications Setting** area, click ![add](image).
   
   You can configure the network devices in the service group to send SNMP messages to one or more notification receivers (e.g., a network management system).

8 Configure the settings in the **Notification Settings** dialog box.

9 Click **OK**.
   
   The agent appears in the **Notification Setting** list.

10 If you are using SNMPv3, click **Add** in the **Security User** area to add a security user.
   
   Security users are only required if you are using SNMPv3. If you are not using SNMPv3, you can skip these steps.

11 Configure the settings in the **Add Security User** dialog box.

12 Click **OK**.
   
   The user is displayed in the **Notification Users** list.

13 When finished configuring SNMP, click **OK**.

**Related Topics**

- **Agent Settings**
- **Notification Settings**
- **Adding Security User Settings**

**Agent Settings**

Configure the settings in the **Agent Settings** area.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **SNMP Version** | Specifies the version of SNMP you want to use.  
  v2c–Used for standard models. Uses community-based authentication.  
  v3–Used when you want a high security model. Requires a security user for notifications. |
| **Transport**    | Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocols:  
  TCP–This protocol has error-recovery services, which assures message delivery, and messages are delivered in the order they were sent. Some SNMP managers only support SNMP over TCP.  
  UDP–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. |
| **Port**         | Specifies the port that the RealPresence Resource Manager system uses for general SNMP messages. By default, the RealPresence Resource Manager system uses port 161. |
Managing Service Groups

Notification Settings
Configure the settings in the Notification Settings dialog box.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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. The RealPresence Resource Manager system has only one valid context (public by default), which is identified by the Community 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>Local Engine Id</td>
<td>For SNMPv3 only. Displays the RealPresence Resource Manager system contextEngineID for SNMPv3.</td>
</tr>
<tr>
<td>Security User</td>
<td>For SNMPv3 only. Specifies the security name required to access a monitored MIB object. You must first add a security user before you can select a user from the drop-down list. This name cannot be snmpuser.</td>
</tr>
</tbody>
</table>

### Notification Settings
Configure the settings in the Notification Settings dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable agent</td>
<td>Select to enable the notification agent. Clear to stop using this agent without deleting it.</td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol for SNMP communications to the host receiver (TCP or UDP).</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the host receiver (the SNMP manager to which this agent sends notifications).</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the RealPresence Resource Manager system uses to send notifications. Default port–162</td>
</tr>
<tr>
<td>Notification type</td>
<td>The type of notification that this agent sends to the notification receiver:</td>
</tr>
<tr>
<td></td>
<td>• Inform–The agent sends an unsolicited message to a notification receiver and expects or requires the receiver to respond with a confirmation message.</td>
</tr>
<tr>
<td></td>
<td>• Trap–The agent sends an unsolicited message to a notification receiver and does not expect or require a confirmation message.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>The version of SNMP used for this agent (v2c or v3).</td>
</tr>
<tr>
<td>Security user</td>
<td>For SNMP v3, the user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
</tbody>
</table>

Adding Security User Settings
Configure the settings in the Add Security User dialog box.
Integrate a Service Group with Enterprise Directory

When you integrate a service group with Enterprise Directory, you integrate each network device within the service group with the same Enterprise Directory server and settings.

The Enterprise Directory Integration settings only apply to the following servers in a service group:

- RealPresence DMA
- RealPresence Resource Manager
- RealPresence Web Suite

After you enable the Enterprise Directory integration on RealPresence Web Suite Services Portal, you cannot disable the integration.

To integrate a service group with Active Directory:

1. Go to Network Device > Service Groups.
2. Select the service group you want to configure from Service Group drop-down list in the right corner of the screen.
3. Click Enterprise Directory Integration.
   The Enterprise Directory Integration dialog box displays.
4. Select the Integrate with Enterprise Directory check box.
5 In the **Enterprise Directory Server DNS Name** section, choose one of the following:

- Select the **Auto-discover** radio button to have the systems auto-discover the server by querying DNS.
- Select the **FQDN** radio button and manually input the FQDN enterprise directory server.

6 As needed, configure the enterprise directory integration settings.

7 Click **OK**.

**Related Topics**

*Using Custom Active Directory Attributes*

*Enterprise Directory Integration Settings*

### Enterprise Directory Integration Settings

Configure the enterprise directory integration 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 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>
| Security Level               | The level of security on the connection between the RealPresence Resource Manager system and the enterprise directory server. Possible values include:  
  - **Plain** No security on the connection.  
  - **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. |
| Use LDAP Filter               | Specifies which user accounts to include (an underlying, non-editable filter excludes all non-user objects in the directory). The default expression includes all users that don’t have a status of disabled in the directory. |
| 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. |
Managing a Network Device within a Service Group

The service group map allows you to navigate to any Polycom network device within the service group. When you navigate to a network device to manage it, you can view the web interface for that network device in a new tab on your browser. For example, if you have a RealPresence DMA system within your service group, you can access the RealPresence DMA system from the service group map. The RealPresence DMA system’s web interface displays in a new tab on your browser.

You can manage the following RealPresence products:

- RealPresence DMA
- Polycom RealPresence Access Director
- Polycom RealPresence Collaboration Server
- RealPresence Web Suite Services Portal

To manage a network device from the Service Group map:

2. Within the map area, Select the network device you want to manage.
3. At the top of the screen, click Manage at the top of the screen. The web interface for the selected network device displays on a new tab in your browser.
Service Configuration

This section includes the topics needed to configure services for the RealPresence Resource Manager system video conference scheduling functionality and operations.
Service Integration with a RealPresence DMA System

You can use some RealPresence DMA functions by integrating your RealPresence Resource Manager system with a single RealPresence DMA system.

Once you integrate with RealPresence DMA later than 9.0.x, you can no longer integrate with RealPresence DMA 9.0.x or earlier versions even if you remove the RealPresence DMA later than 9.0.x instance from the RealPresence Resource Manager system.

Integration Overview

The integration provides you with two main functions of the RealPresence DMA system: the Conference Manager function and the Call Server (gatekeeper and SIP proxy/registrar) function.

- Conference Manager
  - Provides a highly reliable and scalable multi-point 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, which can easily be modified.
  - 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 RealPresence DMA 7000 System Operations Guide for more information.

Dedicated User Account for Integration

When you integrate with a RealPresence DMA system you need to use a RealPresence DMA user account to authenticate the RealPresence Resource Manager system with the RealPresence DMA system. This RealPresence DMA user account needs to meet the following requirements:

- Must have the Administrator role.
- Must be assigned gold class of service.
• Must be reserved only for integration with the RealPresence Resource Manager system. You can also use this user account to help you track VMRs created when you schedule pooled conferences. Any created VMRs will be associated with the RealPresence DMA user you use to integrate with the RealPresence Resource Manager system.

**NTP Servers**

It’s important that you configure the RealPresence Resource Manager system and the RealPresence DMA system to use the same NTP server. This ensures that each has the same network time as the other and scheduled conferences start when intended.

**MCU Management**

A Polycom MCU system can be managed by the RealPresence Resource Manager system or the RealPresence DMA system, not both.

If your video network includes MCUs that are managed by both RealPresence Resource Manager and RealPresence DMA, you may want to use a naming convention that includes a qualifier that indicates to the RealPresence DMA system administrator that the MCU is directly registered to the RealPresence Resource Manager system; for example, `ResourceManager_RMX10`.

**Conference Types Supported By the RealPresence DMA system**

When you integrate your RealPresence Resource Manager system with a RealPresence DMA system the following RealPresence Resource Manager system conference types are supported.

• 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 RealPresence DMA system.

• Pooled Conferences are conferences that are scheduled on resources managed by the RealPresence DMA system. Conference templates for pooled conferences are created and maintained on the RealPresence DMA system.

**RealPresence DMA Conference Templates**

You need to have created RealPresence DMA conference templates for schedulers to use when scheduling either a pooled conference (future) or anytime conference. You do this in the RealPresence 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`.  

---

**Polycom, Inc.**
Multi-Tenancy Considerations

RealPresence DMA system conference templates are not area-aware, which means they cannot be associated with a particular area. An area scheduler can select any RealPresence 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 RealPresence 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.

You should plan your site topology with RealPresence DMA system needs in mind. For example, when your RealPresence DMA system uses a supercluster environment, territories have specific functional roles. It’s important to work with your RealPresence DMA system administrator to ensure the site topology meets your environments needs.

When your RealPresence Resource Manager system is integrated with a RealPresence DMA system, you need to configure the primary node of the Resource Manager Default territory to be the appropriate RealPresence DMA cluster after you integrate with a RealPresence DMA system.

See the Polycom RealPresence DMA 7000 System Operations Guide for more information.

Scheduling Capacity

When you integrate your system with a RealPresence DMA system, you can tune the scheduling capacity of the RealPresence DMA system. 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 RealPresence DMA system pool order when scheduling pooled conferences, they rely on an administrator to tune the RealPresence DMA system’s scheduling capacity to ensure efficient use of resources.

There are three ways an administrator can assess RealPresence DMA system scheduling capacity:

- View conference reports from the RealPresence 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 individual conferences.

Polycom recommends setting the RealPresence DMA system scheduling capacity more conservatively at first and then tuning for increased conference activity.

Integrating with a RealPresence DMA Supercluster

You can integrate with a RealPresence DMA system deployed as a supercluster that uses single-node or dual-node clusters.
Integrating with a RealPresence DMA system

After your system is integrated with a RealPresence DMA, the RealPresence Resource Manager automatically detects any changes to the RealPresence DMA system’s superclusters without needing to re-integrate.

RealPresence Resource Manager system users with the Device Administrator role can add a RealPresence DMA system to a RealPresence Resource Manager system.

Requirements of Dedicated RealPresence DMA User Account

When you integrate with a RealPresence DMA system, you need to create a dedicated RealPresence DMA user account to authenticate the RealPresence Resource Manager system with the DMA system. This DMA user account needs to meet the following requirements:

- Must have the Administrator role.
- Must be assigned gold class of service.
- Must be reserved only for integration with the RealPresence Resource Manager system.

For more information on creating user accounts for the RealPresence DMA system, see the Polycom RealPresence DMA System Operations Guide.

Add a RealPresence DMA system by IP Address

You need to integrate with the RealPresence DMA system by adding it to your RealPresence Resource Manager system. You can add a single RealPresence DMA system for service integration and license management. A local RealPresence DMA system cluster can also be added to RealPresence Resource Manager for service integration.

You should be a Device Administrator for the RealPresence Resource Manager system. And your RealPresence DMA system is reachable via ICMP.

You can add a RealPresence DMA system by IP address, and choose to use RealPresence Resource Manager to do the license management or not from the License Configuration tab.

If you work in vCenter environment, see Appendix A: Working in a vCenter Environment on how to add new or existing RealPresence DMA instance by provider.

To add a RealPresence DMA system by IP address:

1. Go to Network Device > Instances and click Add.
2. Select RealPresence DMA as Device Type.
3. Select IP or FQDN Address in the Add By drop-down list.
4. Specify the parameters in the table below.
5. Click the Servers tab to specify a RealPresence DMA HA cluster if needed.
6. In the Available section, select the server(s) and click the arrow icon to move the list to the Selected section.
7  Select the two servers in the Selected section.
8  Click **OK**. RealPresence Resource Manager will search the RealPresence DMA system. If it cannot find the RealPresence DMA system, it will report an error.
    The RealPresence DMA system appears in the **Network Instance** list.

**Related Topics**

*Scheduling Capacity*

*Working in a vCenter Environment*

*Polycom RealPresence DMA Integration Settings*

**Polycom RealPresence DMA Integration Settings**

Configure the settings for RealPresence DMA integration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Type</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the RealPresence DMA system.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the RealPresence DMA system.</td>
</tr>
<tr>
<td>Management Address</td>
<td>The virtual IP address or FQDN for the RealPresence DMA system. For RealPresence DMA systems with multiple clusters, indicate the FQDN or virtual IP of the cluster you want to use. If your RealPresence DMA system is configured for a supercluster, be sure to use the Virtual IP address for a cluster that is co-located with the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Admin User</td>
<td>The RealPresence DMA system user you use to authenticate the RealPresence DMA system must have the Administrator role and gold class of service. You should use a RealPresence DMA user that is reserved only for integration with the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Admin Password</td>
<td></td>
</tr>
</tbody>
</table>

**Service Integration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider-side Proxy IP Address</td>
<td>If RealPresence DMA works as a software-based edge server, select this check box and enter the proxy IP address. Only RealPresence DMA versions later than 9.0.x supports this feature. See the <em>RealPresence DMA Release Notes</em> available on the Polycom Support Center for the supported RealPresence DMA versions.</td>
</tr>
<tr>
<td>Integrate RealPresence DMA system’s conference manager and call server services with RealPresence Resource Manager system’s conferencing and endpoint services</td>
<td>Select this check box to enable service integration.</td>
</tr>
</tbody>
</table>
Configure the Default Territory

You should configure the Resource Manager Default territory to be the primary RealPresence DMA cluster after you integrate with a RealPresence DMA system.

To configure the default territory:

1. Go to Network Topology > Territories.
2. Select the Default Resource Manager Territory.
3. Click Edit.
4. In the Edit Territory dialog, select a RealPresence DMA cluster to use from the Primary Cluster drop-down list.
5. Click OK.

Managing a RealPresence DMA System

If your RealPresence Resource Manager is integrated with a RealPresence DMA system, you can view details about the system, edit the integration settings, as well as delete the integration.

Edit a RealPresence DMA system

You can edit the properties of an integrated RealPresence DMA system.

You must have the Device Administrator role in order to edit a RealPresence DMA system.
To edit a RealPresence DMA system:

1. Go to **Network Device > Instances**.
2. Select the RealPresence DMA system and click **Edit**.
3. In the **Edit DMA** dialog, edit the properties of the RealPresence DMA system.
4. Click **OK**.

**Stop the Service Integration for a RealPresence DMA system**

You can disintegrate a RealPresence DMA system from the RealPresence Resource Manager system. When you do this, you can no longer use the DMA Pool Orders associated with the RealPresence DMA system for conferences. In addition, DMA-synced endpoints that have not been associated with users can no longer be monitored or managed by the RealPresence Resource Manager system.

You must have the Device Administrator role.

To delete a RealPresence DMA system from a RealPresence Resource Manager system:

1. Go to **Network Device > DMA**.
2. Select the RealPresence DMA system and click **Delete**.
3. Click **OK** to confirm the deletion.

**Working with RealPresence DMA Pool Orders**

When the RealPresence Resource Manager system is configured to work with a RealPresence DMA system, conference schedulers can schedule conferences on RealPresence DMA system pool orders. DMA Pool Orders are groups of MCU pools that are hierarchically organized.

RealPresence DMA system pool orders associated with your configured RealPresence DMA system are automatically displayed in the RealPresence Resource Manager system.

The RealPresence DMA system administrator is responsible for setting up pool orders to be used. You should work with your RealPresence DMA system administrator to determine the specifics about the pool orders associated with your RealPresence DMA system. This information can also be useful for schedulers who need to choose a pool order to use for a conference.

You cannot modify any properties of these pool orders through the RealPresence Resource Manager system.

Some uses for RealPresence DMA system pool orders:

- The RealPresence 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 RealPresence 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 RealPresence 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*.

### View Details of a RealPresence DMA system Pool Order

After you integrate your RealPresence Resource Manager system with a RealPresence DMA system, you can view RealPresence DMA system pool orders that are available for scheduling. For example, you can see how many ports are available in a pool order.

**To view details a RealPresence DMA system Pool Order:**

1. Go to Network Device > Instances.
2. Select a RealPresence DMA from the list.
3. Click More > DMA Pool Orders.
   - The DMA Pool Order Details dialog lists the details for pool orders on the selected RealPresence DMA system. These details are configured on the RealPresence DMA system and cannot be modified with the RealPresence Resource Manager system.
4. Click Close.

**Related Topics**

DMA Pool Order Details

### DMA Pool Order Details

The DMA Pool Order Details dialog lists the details for pool orders on the selected RealPresence DMA system.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name to identify the RealPresence DMA system Pool Order.</td>
</tr>
<tr>
<td>Actual Capacity</td>
<td>The total number of ports included in this RealPresence DMA system Pool Order.</td>
</tr>
<tr>
<td>Scheduling Capacity</td>
<td>The number of ports available to schedule for this RealPresence DMA system Pool Order. This number matches the scheduling capacity percentage that was configured for this RealPresence DMA system.</td>
</tr>
</tbody>
</table>
Associate a RealPresence DMA system Pool Order with an Area

When you associate a pool order with a specific area, only users belonging to that area (or able to manage the area) can schedule conferences for that RealPresence DMA system pool order.

You need the Device Administrator role to associate a DMA pool order with an area. Schedulers and area schedulers cannot select particular resources on which to schedule conferences.

To associate a RealPresence DMA system Pool Order with an Area:

1. Go to Network Device > Instances.
2. Select a RealPresence DMA from the list.
3. Click More > DMA Pool Orders.
4. Select the DMA Pool Order of interest and click Associate Areas.
5. In the Available Areas section, select and move the desired area(s) to Selected Areas list. You can move the unwanted are(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 RealPresence DMA system pool order with an area. The Available Areas list is limited to the areas that you manage.
6. Click OK.

Working with Endpoints Synchronized from a RealPresence DMA System

After integrating with the RealPresence Resource Manager system, the RealPresence DMA-registered endpoints are synchronized to the RealPresence Resource Manager system.

H.323 endpoints registered with the RealPresence DMA system's gatekeeper automatically display in a RealPresence Resource Manager system that has been configured with a RealPresence DMA system, using both the RealPresence DMA system's call server and conference manager. This allows you to track the endpoints registered to the RealPresence DMA system.

Once RealPresence DMA-registered endpoints are synchronized to the RealPresence Resource Manager system, you can include them in scheduled management operations such as provisioning and scheduled software updates. RealPresence DMA-registered endpoints are synchronized daily at 1 a.m. to ensure that endpoint data remains consistent between the RealPresence DMA system and the RealPresence Resource Manager system. You can also modify the properties of RealPresence DMA system-synced endpoints.

If you want to schedule the RealPresence DMA endpoint in a conference, you must first associate the endpoint with a user.

When you take any of the following actions for a RealPresence DMA system-synchronized endpoint, RealPresence Resource Manager system considers the endpoint to be a non-dynamically managed endpoint:

- Include the endpoint in a scheduled provisioning (may happen automatically)
- Include the endpoint in a scheduled software update
- Modify the properties of the endpoints (including associating a user)
- Add the endpoint to an address book

If the RealPresence DMA administrator deletes an endpoint from the RealPresence DMA system, it will also be cleared from displaying in the RealPresence Resource Manager system. RealPresence DMA-synchronized endpoints that you have associated with a user, scheduled in a conference, or provisioned will not be cleared during a RealPresence DMA action. Endpoints that you have started to manage in any way are seen by RealPresence Resource Manager as managed endpoints. If you want to remove them, you need to do so using the RealPresence Resource Manager system.

Each synchronized RealPresence DMA-registered endpoint consumes a video endpoint license in the RealPresence Resource Manager system.

**Unique H.323 Aliases Required**

In order for a RealPresence DMA-registered endpoint to synchronize and display in the RealPresence Resource Manager system, it must have a unique H.323 alias. If any managed endpoint in the RealPresence Resource Manager system has the same H.323 alias as a RealPresence DMA-registered endpoint, the DMA-registered endpoint information will not display.

There is no automatic way to ensure unique H.323 aliases between RealPresence DMA-registered endpoints and endpoints directly managed by the RealPresence Resource Manager system. To determine if there is any overlap, you can export a list of the user-reserved H.323 aliases from the RealPresence Resource Manager system and do a comparison with those listed in your RealPresence DMA system. For more information on exporting user dialing information, see Export User Aliases.

SIP-only endpoints that register with the RealPresence DMA system instead of the RealPresence Resource Manager system’s provisioning service do not display in the RealPresence Resource Manager system. You must manually add them to the RealPresence Resource Manager system in order to manage the endpoints.

**Monitor RealPresence DMA-Synchronized Endpoints**

You can monitor H.323 endpoints that are synchronized from the RealPresence DMA system.

To monitor RealPresence DMA-synchronized endpoints:

1. Go to Endpoint > Monitor View.
2. Use the Mode column to determine if an H.323 endpoint has been synchronized from the RealPresence DMA system. RealPresence DMA-synchronized endpoints display with the following icon: Synced RealPresence DMA Endpoints.
3. Optionally, you can filter the endpoint list to include only RealPresence DMA-Synced Endpoints.
   a. Click Filter.
   b. Click the Type box and select DMA-Synced Endpoints from the displayed list.
Schedule RealPresence DMA-Synchronized Endpoints in Conferences

If you associated a RealPresence DMA-synced endpoint with a user or room, you can also schedule that associated endpoint in conferences when you schedule that user or room.

To associate an endpoint to a user:

1. Go to Endpoint > Monitor View.
2. As needed, click Filter to customize the Endpoint list.
3. Select the endpoint of interest.
4. Click More > Associate User.
5. In the Last Name or Room Name field of the Associate User dialog, enter all or part of the user’s last name and click Search.
   - The system displays the list of user or rooms that meet your search criteria.
6. Select the user of interest and click Close.

Related Topics
- Configure Conferencing

Licensing Threshold for RealPresence DMA-Synchronized H.323 Endpoints

H.323 endpoints registered to the RealPresence DMA system's gatekeeper are synchronized to the RealPresence Resource Manager system as soon as you integrate your system with a RealPresence DMA system for both conference management and call server functions. These endpoints can be Polycom endpoints with full management capacity or third-party endpoints with limited management capacity in the RealPresence Resource Manager system. To avoid consuming too many device licenses by third-party endpoints, the RealPresence Resource Manager system has two thresholds to limit the number of RealPresence DMA-synced endpoints you can monitor.

Threshold for Stopping Synchronization

The RealPresence Resource Manager system will stop synchronizing RealPresence DMA-synced endpoints when 80% of your device licenses have been consumed. The left 20% capacity is reserved for endpoints managed in other modes.

You can contact Polycom Support to change the threshold.

See View the Endpoint List for endpoint management modes.
Threshold for Deleting Inactive Synchronized H.323 Endpoints

The RealPresence Resource Manager system automatically deletes inactive RealPresence DMA-synchronized endpoints when the total used device licenses exceeds 90%. This ensures that you always have enough device licenses for active and dynamically-managed endpoints. An endpoint is considered inactive when the RealPresence Resource Manager system detects that it is not registered with the gatekeeper, the directory, Exchange, or the presence service.
Service Integration with Session Border Controllers

You can integrate Session Border Controllers service with RealPresence Resource Manager to perform network device management tasks.

Supported Session Border Controllers

The RealPresence Resource Manager system supports three types of session border controllers for specific signaling.

The supported session border controllers are:

- Acme SBC (SIP endpoints only)
- Polycom VBP (H.323 endpoints only)
- RealPresence Access Director (both SIP and H.323 endpoints)

Managing Polycom VBP Devices

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, 6400, or 7301 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.

Add a Polycom VBP Device

You can add a Polycom VBP device to the RealPresence Resource Manager system.

To add a Polycom VBP device:

1. Go to Network Device > Instances.
2. Click Add.
3. Select VBP from the Device Type drop-down list.
4. Configure the settings for adding a Polycom VBP device.
5 Click OK.

You can also choose 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 as described in the next topic.

Adding Polycom VBP Settings
Configure the settings for adding a Polycom VBP device.

<table>
<thead>
<tr>
<th>Settings</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 Proxy IP Address</td>
<td>The Private Network IP address for the Polycom VBP device.</td>
</tr>
<tr>
<td>Subscriber-side IP Address</td>
<td>The Public Network IP address for the Polycom VBP device.</td>
</tr>
</tbody>
</table>

Edit a Polycom VBP Device
You can edit the settings of a Polycom VBP device.

To edit a Polycom VBP device:
1 Go to Network Device > Instances.
2 Click Filter and select VBP as Device Type.
3 Select the Polycom VBP device of interest and click Edit.
4 Configure these settings as needed in the Edit Instance dialog.
5 Click OK.

Delete a Polycom VBP Device
You can delete a Polycom VBP device from the RealPresence Resource Manager system.

To delete a Polycom VBP device:
1 Go to Network Device > Instances.
2 Click Filter and select VBP as Device Type.
3 Select the Polycom VBP device of interest and click Delete.
4 Click Yes to confirm the deletion.

Identify Endpoints Using the Polycom VBP Device
This procedure identifies only Polycom® HDX® systems, Polycom® RealPresence® Group Series, Polycom CMA Desktop, Polycom RealPresence Mobile, Polycom® RealPresence Desktop, Polycom® RealPresence Debut™, and Polycom® VVX® systems have the following characteristics:
Service Integration with Session Border Controllers

- Registered to the RealPresence Resource Manager system
- Using the Polycom VBP firewall
- Are dynamically managed

A Polycom HDX or legacy endpoint system in scheduled 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 scheduled 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 Filter and select IP Address.
3. Enter the provider-side IP address of the Polycom VBP device and press Search.

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.

Managing a Polycom RealPresence Access Director System

With the RealPresence Access Director system, Polycom offers a software-based edge server to securely route communication, management, and content through firewalls without requiring special dialing methods or additional client hardware or software.

If your video infrastructure environment includes a RealPresence Access Director system, you must ensure that your RealPresence Resource Manager system is aware of the RealPresence Access Director system. You need to either dynamically manage or manually add the RealPresence Access Director system to your RealPresence Resource Manager system. See Dynamically Managing a RealPresence Access Director System for details.

Manually Add a RealPresence Access Director System

If you are not going to dynamically manage the RealPresence Access Director system, you can manually add it to the RealPresence Resource Manager system.

When you manually add a RealPresence Access Director system, you will not be able to monitor its status or view any call information for calls routed from the RealPresence Access Director system.

When you use the RealPresence Resource Manager system to dynamically manage a RealPresence Access Director system, you should not manually add it to your system.
To manually add a RealPresence Access Director system:

1. Create a site that includes the subnet on which the RealPresence Access Director system resides. You cannot use the same site for more than one RealPresence Access Director system. You must create a unique site for each RealPresence Access Director system that you use.
2. Go to Network Device > Instances and click Add .
3. Select RealPresence Access Director from the Device Type drop-down list.
4. Select IP or FQDN Address from the Add By drop-down list.
5. Configure the settings for adding a RealPresence Access Director system.
6. In the Service Integration tab, specify the Provider-side Proxy IP Address.
7. Click OK.

Related Topics
Add a Site
Adding a RealPresence Access Director System Settings

Adding a RealPresence Access Director System Settings
Configure the settings for adding a RealPresence Access Director system.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the RealPresence Access Director system.</td>
</tr>
<tr>
<td>Version</td>
<td>The version number of the RealPresence Access Director system that you are going to add.</td>
</tr>
<tr>
<td>Management Address</td>
<td>The Private Network IP address for the RealPresence Access Director system.</td>
</tr>
<tr>
<td>Admin User/Password</td>
<td>The user name and password of the RealPresence Access Director system.</td>
</tr>
</tbody>
</table>

Managing SBC Devices
Polycom supports the use of the Acme Packet Net-Net Enterprise Session Director session border control with the RealPresence Resource Manager system.

Add an SBC Device
You can add an SBC device to the RealPresence Resource Manager system.

To add an SBC device:

1. Go to Network Device > Instances and click Add .
2. Select Acme SBC from the Device Type drop-down list.
3. Select IP or FQDN Address from the Add By drop-down list.
4 Configure the settings for adding an SBC device.
5 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.

Adding an SBC Device Settings

Configure the settings for adding an SBC device.

<table>
<thead>
<tr>
<th>Field</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 Proxy IP Address</td>
<td>The Private Network IP address for the SBC device.</td>
</tr>
<tr>
<td>Subscriber-side Proxy IP Address</td>
<td>The Public Network IP address for the SBC device.</td>
</tr>
</tbody>
</table>

Edit an SBC Device

You can edit the settings of an SBC device.

To edit an SBC device:
1 Go to Network Device > Instances.
2 Select the SBC device of interest and click Edit.
3 Configure the settings as needed in the Edit SBC dialog.
4 Click OK.

Delete an SBC Device

You can delete an SBC device from the RealPresence Resource Manager system.

To delete an SBC device from a RealPresence Resource Manager system:
1 Go to Network Device > Instances.
2 Select the SBC device of interest and click Delete.
3 Click OK to confirm the deletion.

Identify Endpoints Using the SBC Device

You can identify Polycom HDX systems, Polycom Group Series, and RealPresence Mobile clients that are dynamically managed by the RealPresence Resource Manager system or using the SBC device.
To identify which endpoints are using the SBC firewall:

1. Go to Endpoint > Monitor View.
2. Click 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.
Service Integration with Bridges

The Polycom RealPresence Resource Manager system can manage and monitor Polycom MCUs.

Add an MCU Manually

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.

Polycom MGC systems may only have H.323/H.320 services.

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 refresh the device.

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.

Polycom RealPresence Collaboration Server (RMX) systems cannot be managed by two management systems at the same time. When your deployment includes a Polycom RealPresence DMA system, you can manage an RealPresence Collaboration Server (RMX) system either in the RealPresence DMA system or with the RealPresence Resource Manager, not both. Back-end communication with the Polycom RealPresence Collaboration Server (RMX) system control units and IP service blades must be enabled.

To add an MCU bridge or find an MCU on the network:

1. Go to Network Device > Instances and click Add.
2. In the Add Instance dialog, select RealPresence Collaboration Server or MGC as Device Type.
3. Select IP &FQDN Address from the Add By drop-down list.
4. Enter a Name for this instance.
   - If your system integrates with a Polycom RealPresence DMA system, make sure your MCU system name includes a qualifier that indicates to the RealPresence DMA system administrator that the MCU is directly registered to the RealPresence Resource Manager system; for example, ResourceManager_RMX10.
5. Specify the version of the MCU product in the Version field.
6. Specify the MCU Management Address.
7. Enter the Admin User and Admin Password for the MCU.
8. Click OK.
9 Indicate how you are integrating the MCU service.
   If you want to integrate the MCU with RealPresence Resource Manager conferences instead of the
   RealPresence DMA system, check the Conference Controlled by Resource Manager check box.
10 Complete the Identification, Addresses, Capabilities, MCU Resources, and MCU Cascading
    sections.
    Pay particular attention to the Capabilities options, because these settings determine how the MCU
    is used.
11 Click OK.
   The RealPresence Resource Manager system will find the MCU on the network.
   If the RealPresence Resource Manager system cannot find the MCU on the network, an Error dialog
   appears.
   If the MCU is added successfully, it will appear in the Network Device list. By default, the system:
   ➢ Adds the MCU to the applicable site.
   ➢ Sets the HTTP Port to 80.
   ➢ Makes the MCU Available to Schedule.

Conference Scheduling Requirements
To schedule conference, you need to define network services and change the default entry queue setting.
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.
Additionally, you must change the default entry queue setting to “standard lobby”. The default entry queue
mode is “ad hoc”. “Ad hoc” cannot be used because it allows participants to join and start a conference
before start time and consume the conference ID that is reserved for the RealPresence Resource Manager
system. Scheduled participants must be held in the standard lobby until the start time of the direct
conference to ensure the conference uses a valid conference ID.

Edit an MCU
You can edit a managed MCU.

To edit an MCU from the RealPresence Resource Manager system:
1 Go to Network Device > Instances.
2 As needed, click Filter  and select RealPresence Collaboration Server or MGC as Device
   Type to customize the MCU list.
3 Select an MCU and click Edit .
4 Complete the Identification, Addresses, Capabilities, MCU Resources, and MCU Cascading
   sections of the Edit Instance dialog.
   At a minimum, assign the MCU a Name.
5 Click OK.
Optionally, you can refresh the MCU to use the settings from the MCU itself. To do this, click.

**Related Topics**

View MCU Ports

MCU Settings

**MCU Settings**

Edit the MCU settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification</strong></td>
<td></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>• The name must be in ASCII only and may have an unlimited number of</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>MCU registered with the gatekeeper and it is a third-party system. In</td>
</tr>
<tr>
<td></td>
<td>other cases, it is the system name, which might be different than the H.323</td>
</tr>
<tr>
<td>Description</td>
<td>A free-form text field (Extended ASCII only) in which information about the</td>
</tr>
<tr>
<td></td>
<td>MCU can be added</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number (ASCII only) of the MCU. The serial number displays if</td>
</tr>
<tr>
<td></td>
<td>the MCU is 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</td>
</tr>
<tr>
<td></td>
<td>provides the version number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>HTTP URL</td>
<td>(Polycom RealPresence Collaboration Server (RMX) systems only)</td>
</tr>
<tr>
<td></td>
<td>The management URL for the endpoint, if available (ASCII only). This URL</td>
</tr>
<tr>
<td></td>
<td>enables the RealPresence Resource Manager system to start the endpoint ’s</td>
</tr>
<tr>
<td></td>
<td>management system using the Manage function.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>(Polycom RealPresence Collaboration Server (RMX) systems only)</td>
</tr>
<tr>
<td></td>
<td>The HTTP port number for the MCU communications. The MCU provides the port</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>uses port 80 and in secure (HTTPS) mode, the RealPresence Collaboration</td>
</tr>
<tr>
<td></td>
<td>Server uses port 443.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assign Area</td>
<td>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>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>• IP (H.323) - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP.</td>
</tr>
<tr>
<td></td>
<td>• ISDN (H.320) - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.</td>
</tr>
<tr>
<td></td>
<td>• IP (SIP) - A standard that defines the protocols used for multimedia communications on SIP networks.</td>
</tr>
<tr>
<td></td>
<td>The MCU automatically provides the protocols if it registered successfully or is managed.</td>
</tr>
<tr>
<td></td>
<td>Polycom MGC systems may only have H.323/H.320 services.</td>
</tr>
<tr>
<td>Capabilities Enabled</td>
<td>Capabilities to enable on this MCU. Options are:</td>
</tr>
<tr>
<td></td>
<td>• MCU - The device can act as a control unit for multipoint conferences.</td>
</tr>
<tr>
<td></td>
<td>• Available to Schedule - Select this option to make the MCU available to users who are scheduling conferences.</td>
</tr>
<tr>
<td>MCU Resources</td>
<td></td>
</tr>
<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>(Not available for MGC systems)</td>
</tr>
<tr>
<td></td>
<td>Maximum number of video ports available on the MCU.</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 MGC device supports an IVR.</td>
</tr>
<tr>
<td>Entry Queue Numeric ID</td>
<td>The IP 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 ISDN number that conference participants dial to access the IVR prompt to join a conference.</td>
</tr>
</tbody>
</table>
Delete an MCU Bridge

When you delete an MCU from the system, it is no longer managed and cannot be used on conferences.

To delete an MCU from the RealPresence Resource Manager system:

1. Go to Network Device > Instances.
2. As needed, click Filter and select RealPresence Collaboration Server or MGC as Device Type to customize the MCU list.
3. Select the MCU of interest and click Delete.
4. Click OK to confirm the deletion.

The MCU list is updated.

View Device Details

You can view details about a managed MCU.

To view detailed information about a managed MCU:

1. Go to Network Device > Instances.
2. As needed, click Filter and select RealPresence Collaboration Server or MGC as Device Type to customize the MCU list.
3. Select the MCU of interest.
4. Click View Details to view detailed information.
5. Click Alert beside the integrated MCU to view its alerts if any.
6. Select your interested item from the More drop-down list to view other information.
**View Bridge Hardware**

You can view the hardware properties of a managed MCU.

To view the hardware configuration of an MCU:

1. Go to **Network Device > Instances**.
2. As needed, click **Filter** and select **RealPresence Collaboration Server** or **MGC** as Device Type to customize the MCU list.
3. In the MCU list, select the bridge of interest and click **View Hardware** from the **More** drop-down list.

   A **Hardware** pane appears. 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 MCU Services**

You can view the services provided by a managed MCU.

To view the network services available on the MCU:

1. Go to **Network Device > Instances**.
2. As needed, click **Filter** and select **RealPresence Collaboration Server** or **MGC** as Device Type to customize the MCU list.
3. In the MCU list, select the bridge of interest and click **View Services** from the **More** drop-down list.

   A **Services** pane appears. It lists the network services for the selected bridge and identifies the **Service Type**, **Service Name**, and the default setting for the network service.

**View MCU Conferences**

You can view the conferences hosted by an MCU.

To view information about the conferences resident on an MCU:

1. Go to **Network Device > Instances**.
2. As needed, click **Filter** and select **RealPresence Collaboration Server** or **MGC** as Device Type to customize the MCU list.
3. In the MCU list, select the bridge of interest and click **View Conferences** from the **More** drop-down list.

   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**, and **Creator**.

   A user can only view area-specific information for an area(s) that he has permission to manage.
View MCU Ports

The RealPresence Resource Manager system reports port numbers based on resource usage for CIF calls. Version 8.1 and later Polycom MCUs report port numbers based on resource usage for HD720p30 calls. In general, 3 CIF = 1 HD720p30, but it varies depending on bridge/card type and other factors.

See your RealPresence Collaboration Server (RMX) system documentation for more detailed information about resource usage.

This option is not available for Polycom MGC systems.

To view information about the MCU ports:

1. Go to Network Device > Instances.
2. As needed, click Filter ▼ and select RealPresence Collaboration Server or MGC as Device Type to customize the MCU list.
3. In the MCU list, select a bridge and click View Ports from the More drop-down list.
   A Ports pane appears. It lists the ports for the selected bridge and identifies the Audio Ports Available, CIF Ports Available, Audio Ports in Use, and CIF Ports in Use.

View MCU Meeting Rooms

You can view information about available meeting rooms:

To view information about meeting rooms:

1. Go to Network Device > Instances.
2. As needed, click Filter ▼ and select RealPresence Collaboration Server or MGC as Device Type to customize the MCU list.
3. In the MCU list, select the bridge of interest and click View Meeting Rooms from the More drop-down list.
   A Meeting Rooms pane appears. It lists the meeting rooms for the selected bridge and identifies the meeting room by Name, ID, Duration, Conference Password, Chairperson Password, and Profile.

View MCU Entry Queues

You can view information about the available entry queues available on a managed MCU.

To view information about entry queues:

1. Go to Network Device > Instances.
2. As needed, click Filter ▼ and select RealPresence Collaboration Server or MGC as Device Type to customize the MCU list.
3 In the MCU list, select the bridge of interest and click View Entry Queues from the More drop-down list.

An Entry Queues pane appears. 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

You can view information about gateway conferences on a managed MCU.

**To view information about gateway conferences:**

1. Go to Network Device > Instances.
2. As needed, click Filter and select RealPresence Collaboration Server or MGC as Device Type to customize the MCU list.
3. In the MCU list, select the bridge of interest and click View Gateway Conferences from the More drop-down list.

A Gateway 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, and Creator.
Configure Conferencing

The RealPresence Resource Manager system can schedule, manage, and monitor video conferences.
Setting Up Site Topology

You can edit the default RealPresence Resource Manager system topology settings to support your company’s network topology.

Understanding Site Topology

Site topology information describes your network and its interfaces to other networks. It includes 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 RealPresence Resource Manager system is responsible.

The site topology you create within the RealPresence 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 system is integrated with a Polycom RealPresence DMA system, the RealPresence DMA system inherits all site topology settings from the RealPresence Resource Manager. Be sure to consult with your RealPresence DMA system admin before making any changes, see Considerations for Site Topology in the Multi-Tenancy Considerations section.

- 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 are not 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.

Related Topics
Considerations for Site Topology

Managing Sites
Sites are the primary way you organize your video and audio network.
The Network Topology > Sites page can display up to 1000 sites. For audio users, you can apply different configuration profiles to different sites when you provision.
If there are more than 500 sites, the system does not display the Dashboard > Site Map pane and the Site Topology map. The Site-Links, Site-to-Site Exclusions, Network Clouds, Territories, Reports > Site Statistics, Reports > Site-Links Statistics, and RealPresence DMA integration are not supported.

Related Topics
Network Provisioning Profiles

View the Graphical Site Topology
The RealPresence 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.

To view the graphical site topology:
» Go to Network Topology > Site Topology.
The Site Topology page appears. It graphically displays the sites and site links defined to the RealPresence Resource Manager system.
➢ Hover over a map element to view information about it.
Setting Up Site Topology

- 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.
- Click Filter to filter (by site name, territory name, IP address, network devices, and alerts) which sites are displayed on the map.

**View the Sites List**

The Network Topology > Sites page contains a list of the sites defined to the RealPresence Resource Manager system. This page can show up to 1000 sites.

**To view the Sites list:**

1. Go to Network Topology > Sites.
2. Filter the sites by Site Name. You can search the sites by entering a site name in the Search field. The Sites list appears.

**Related Topics**

Site Details

**Site Details**

The Sites list includes this information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site 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, 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>
<tr>
<td>Max Bit Rate (Kbps)</td>
<td>The per-call bandwidth limit for audio and video calls.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory to which the site belongs, which determines the RealPresence Resource Manager system responsible for it.</td>
</tr>
</tbody>
</table>

**Add a Site**

You can define a new site in the system’s site topology and specify which subnets are associated with it. You can define overlapping subnets within a site or between sites. Larger subnets can contain smaller ones. When the system determines which subnet a given IP address belongs to, it chooses the subnet with the longest IP match.
Setting Up Site Topology

For example:

Subnet1 = 10.0.0.0/8
Subnet2 = 10.33.24.0/24

The IP address 10.33.24.70 belongs to subnet2, while the IP address 10.22.23.70 belongs to subnet1.

To add a site:

1. Go to Network Topology > Sites or Network Topology > Site Topology.
   - To add a site in the Sites page, Click Add.
   - To add a site in the Site Topology page, go to Site Actions > Add.
2. In the Add Site dialog, enter a Site Name and Description for the site.
3. Complete the General Info, H.323 Routing, SIP Routing, Subnet, and if applicable ISDN Number Assignment, sections of the Add Site dialog. The minimum information required is Site Name, Description, Location, and Subnets.
4. Click OK.

Related Topics

Site Settings

Site Settings

Configure the following site settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td></td>
</tr>
<tr>
<td>Site Name</td>
<td>A meaningful name for the site, this name can be 64 characters (ASCII only)</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description (ASCII only) of the site.</td>
</tr>
<tr>
<td>Enable Mutual TLS</td>
<td>Enable Mutual TLS</td>
</tr>
<tr>
<td>Override ITU Dialing Rules</td>
<td>Check this box to override the standard dial rules established by the</td>
</tr>
<tr>
<td></td>
<td>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,</td>
</tr>
<tr>
<td></td>
<td>the city code for Paris is 01, 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,</td>
</tr>
<tr>
<td></td>
<td>subscriber numbers may have seven digits or ten digits depending upon the</td>
</tr>
<tr>
<td></td>
<td>region.</td>
</tr>
</tbody>
</table>
Setting Up Site Topology

### Assignment Method

The ISDN number assignment method for the site. Possible values include:
- **No Auto Assignment**: Select this option when ISDN numbers are not assigned to IP devices.
- **DID (Direct Inward Dial)**: Select this option when you assign a range of phone numbers received from the telephone company service.
- **Gateway Extension Dialing**: 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.

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 RealPresence Resource Manager system.

**Note**

If you do not assign ISDN numbers automatically, you cannot call IP-only endpoints through an ISDN line.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assignment Method</strong></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</td>
</tr>
<tr>
<td></td>
<td>assigned to IP devices.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DID (Direct Inward Dial)</strong>: Select this option when you assign a</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>gateway phone number and a range of extensions (E.164 aliases) that are</td>
</tr>
<tr>
<td></td>
<td>internal to the company. Calls go through a gateway. Endpoints are</td>
</tr>
<tr>
<td></td>
<td>differentiated by the extension at the end of the dial string.</td>
</tr>
<tr>
<td><strong>Territory</strong></td>
<td>Assigns the site to a territory, and thus to a RealPresence Resource</td>
</tr>
<tr>
<td></td>
<td>Manager system.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Specify the geographic location of the site either by longitude + latitude or</td>
</tr>
<tr>
<td></td>
<td>country + city.</td>
</tr>
<tr>
<td><strong>Total Bandwidth (Mbps)</strong></td>
<td>The total bandwidth of the pipe at the site.</td>
</tr>
<tr>
<td><strong>Call Max Bit Rate (kbps)</strong></td>
<td>The maximum bandwidth that can be used for each intrasite call at the site.</td>
</tr>
<tr>
<td></td>
<td>The default and maximum value is 2000000 (2 GB).</td>
</tr>
<tr>
<td><strong>ISDN Number Assignment—</strong></td>
<td><strong>Assignment Method = DID (Direct Inward Dial)</strong></td>
</tr>
<tr>
<td><strong># Digits in Call Line Identifier</strong></td>
<td>Enter the number of digits in the Call Line Identifier (CLID), which is the</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>often 7 for outside local calls, 4 for internal calls, or 11 for callers</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>gatekeeper for address resolution.</td>
</tr>
<tr>
<td><strong># Digits in Short Phone Number</strong></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</td>
</tr>
<tr>
<td></td>
<td>or five digits.</td>
</tr>
<tr>
<td></td>
<td>• This number indicates what part of the dial string is sent to the gate-</td>
</tr>
<tr>
<td></td>
<td>keeper for address resolution in gateway + extension dialing.</td>
</tr>
<tr>
<td><strong>ISDN Number Range - Start</strong></td>
<td>The starting ISDN number to assign automatically to IP devices.</td>
</tr>
<tr>
<td><strong>ISDN Number Range - End</strong></td>
<td>The ending ISDN number to assign automatically to IP devices.</td>
</tr>
</tbody>
</table>

**ISDN Number Assignment—**

**Assignment Method = Gateway Extension Dialing**
### Setting Up Site Topology

**Gateway Phone Number**
- Phone number of the site gateway.

**E164 Start**
- The starting number in a range of available extensions to assign automatically to IP devices.
- 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.

**E164 End**
- The ending number in the range of available extensions to assign automatically to IP devices.

### H.323 Routing

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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></td>
<td><strong>Notes</strong></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 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</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 (IPv4 only) or host name of the SBC or ALG server.</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 string is passed to it. For example, an H.323 Annex O dial string such as <a href="mailto:user@company.com">user@company.com</a> is passed directly to the SBC or ALG instead of resolving company.com to an IP address. Deselect this option if your equipment requires a dial string that is converted from company.com to gatekeeper IP address. This option is appropriate for the Polycom VBP.</td>
</tr>
</tbody>
</table>

### SIP Routing

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables call routing through the Internet.</td>
</tr>
</tbody>
</table>
You can view information about existing sites.

To view information about an existing site:

1. Go to Network Topology > Sites.
2. In the **Sites** page, select a site and go to **More > Site Information**. The **Site Information** dialog appears.

### Related Topics

**Site Information**

The **Site Information** dialog displays the following site information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site 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>Max Bit Rate</td>
<td>The per-call bandwidth limit for 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 <strong>Details</strong> 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 **Network Topology > Sites** or **Network Topology > Site Topology**.
   
   a. In the **Site Topology** page, go to **SITE ACTIONS > Assign Locations**.
   
   b. In the **Sites** page, go to **More > Assign Locations**.

2. In the **Assign Locations to Sites** dialog, select the site of interest by selecting the associated check box and click **Specify Location**.

3. To specify a location by city name:
   
   a. From the **Enter Location By** drop-down list, select **Search for City**.
Setting Up Site Topology

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 matches your query.
d Select the appropriate city using the Country, Division, and Subdivision fields to identify it and click Select.

4 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.

5 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

You can define a new site in the system’s site topology and specify which subnets are associated with it.

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.

To edit settings for a site:
1 Go to Network Topology > Sites or Network Topology > Site Topology.
2 In the Sites list or Site Topology page, select the site of interest and click Edit or SITE ACTION > Edit Site.
3 Edit the General Info, Site Routing, Site Subnet, and if applicable ISDN Number Assignment, sections of the Edit Site dialog.
4 Click OK.

Delete a Site

You can delete a site.
To delete a site:

1. Go to Network Topology > Sites or Network Topology > Site Topology.
2. In the Sites list or Site Topology page, select the site of interest and click Delete or SITE ACTION > Delete.
3. Click OK to confirm the deletion.

Managing Site Links

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.

A link can connect two sites, or it can connect a site to an MPLS network cloud (see Network Clouds).

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 RealPresence Collaboration Server (RMX) profile takes precedence over the bit rate in the conference settings.

View the Site Links List

You can view the list of site links.

To view the Site Links list:

» Go to Network Topology > Site-Links.

The Site-Links list appears.

Related Topics

Site-Links Information

Site-Links Information

The Site-Links list displays the following information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-Link Name</td>
<td>Name of the link</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the link</td>
</tr>
</tbody>
</table>
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 Network Topology > Site-Links.
2. In the Site-Links page, click Add .
3. In the Add Site-Link dialog, enter a Site-Link 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 Network Topology > Site-Links.
2. In the Site-Links list, select the link of interest and Click Edit .
3. In the Edit Site-Link dialog, edit the Site-Link Name, Description, Bandwidth or Max Bit Rate.
4. Click OK.

Delete a Site Link

You can remove site links from the RealPresence Resource Manager system.

Avoid removing a link on which a scheduled conference depends.
To delete a site link:

1. Go to Network Topology > Site-Links.
2. In the Site-Links list, select the site link of interest and click Delete.
3. Click OK to confirm the deletion.

Managing Site-to-Site Exclusions

Create site-to-site exclusions to explicitly deny connection between two sites for audio or video calls.

View the Site-to-Site Exclusion List

You can view a list of site-to-site exclusions.

To view the Site-to-Site exclusion list:

» Go to Network 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 Network Topology > Site-to-Site Exclusions.
2. In the Site-to-Site Exclusions page, click Add.
3. In the Add Site-to-Site Exclusions dialog:
   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 OK.

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

You can delete a site-to-site exclusion.
To delete a site-to-site exclusion:

1. Go to **Network Topology > Site-to-Site Exclusions**.
2. In the **Site-to-Site Exclusions** page, select the exclusion of interest and click **Delete**.
3. Click **OK** to confirm the deletion.

## Territories

A territory is a set of one or more sites for which a RealPresence Resource Manager system is responsible. By default, there is one territory named **Default Resource Manager Territory**, and its primary node (the RealPresence Resource Manager system responsible for it) is set to this system.

You should configure the Resource Manager Default territory to be the primary RealPresence DMA node AFTER you integrate with a RealPresence DMA system.

### View the Territory List

You can view a list of territories.

**To view the Territories list:**

» Go to **Network Topology > Territories**.

The Territories list appears.

### Add a Territory

You can define a new territory in the RealPresence Resource Manager system’s site topology.

**To add a territory:**

1. Go to **Network Topology > Territories**.
2. In the Territories page, click **Add**.
3. Complete the **Territory Info** and **Associated Sites** sections of the **Add Territories** dialog.
4. Click **OK**.

**Related Topics**

[Adding a Territory Settings](#)

**Adding a Territory Settings**

Configure the adding a territory settings.
Edit a Territory

You can edit an existing territory in the RealPresence Resource Manager system’s site topology.

You should configure the Resource Manager Default territory to be the primary RealPresence DMA node AFTER you integrate with a RealPresence DMA system.
To edit a territory:

1. Go to Network 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 as needed.
4. Click OK.

Delete a Territory

You can delete a territory.

To delete a territory:

1. Go to Network Topology > Territories.
2. In the Territories page, select the territory of interest and click Delete.
3. Click OK 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.

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.

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. See View the Sites List to determine the area for a site.

View the List of Network Clouds

You can view the list of network clouds.

To view the Network Cloud list:

» Go to Network Topology > Network Clouds.

The Network Clouds list appears.

Add a Network Cloud

You can add a network cloud.
To add a network cloud:

1. Go to Network Topology > Network Clouds.
2. In the Network Clouds page, click Add.
3. In the Cloud Info section of the Add Network Cloud dialog, enter a unique and meaningful Cloud 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 Filter.
      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.

**Related Topics**

Linked Sites Settings

**Linked Sites Settings**

Configure the linked sites.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Selected Sites</td>
<td>Lists sites linked to the cloud and shows the territory, if any, to which each belongs.</td>
</tr>
</tbody>
</table>

**Edit a Network Cloud**

You can edit the settings of a network cloud.

To edit a network cloud:

1. Go to Network 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 Filter.
      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

You can delete a network cloud.

**To delete a network cloud:**

1. Go to **Network Topology > Network Clouds**.
2. In the **Network Clouds** page, select the network cloud of interest and click **Delete**.
3. Click **OK** to confirm the deletion.
Setting Up the Global Address Book

This section describes how to manage the Global Address Book in the Polycom® RealPresence® Resource Manager system.

The Polycom Global Address Book is a system-managed endpoint directory that enables users with video endpoints to look up and call other users with video endpoints in their video communications network.

View the Global Address Book

You must have the Administrator role and permissions to view the Global Address Book.

To view the Global Address Book:

1. Go to Admin > Directories > Global Address Book.
2. As needed, click Filter to customize the Global Address Book. It can be filtered by Endpoint Name or IP Address.

Related Topics

Global Address Book Information

Global Address Book Information

The user information found in the Global Address Book is listed in the table below.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint 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. The GAB display name is automatically generated when the user is associated with the endpoint. If you want to update the GAB display name, you can do so from the Endpoint &gt; Monitor View.</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>
</tbody>
</table>
Enable or Disable GAB Filter

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.

To enable or disable GAB Filter,
1. Go to Admin > Directories > Global Address Book.
2. Click the Set GAB Filter button.
3. Check or cancel the Disable GAB Filtering to disable or enable GAB Filter.

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.

You must have the Administrator role and permissions, to set or change the Global Address Book password.

To provision this password to endpoints, see Add a Scheduled Provisioning Profile.

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, 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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
Related Topics

Add a Scheduled Provisioning Profile
Using Multiple Address Books

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.

Using Multiple Address Books

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.

Task Overview of Implementing Multiple Address Books

You need to complete the following tasks to implement multiple address books.

RealPresence Resource Manager system users assigned the Administrator role can implement multiple address books.
To implement multiple address books:

1. **Add an Address Book**
   You 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 User Groups**
   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**
   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.

**View the Address Book List and Details**

You can view an address book.

**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 Book Name</td>
<td>Name of the address book.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the address book.</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. The **Address Book** list appears.
Using Multiple Address Books

Address Book Details

The Address Book lists the 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 Book Name</td>
<td>Name of the address book.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the address book.</td>
</tr>
</tbody>
</table>

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 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.
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 User 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**.

8 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**.

9 Click **OK**.

### Adding an Address Book Settings

Complete the fields in the **Add an Address Book** dialog

<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>Address Book 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><strong>Address Book Tiers</strong></td>
<td></td>
</tr>
<tr>
<td>New Tier</td>
<td>Select where you want to add a tier and click to add a new tier to the address book.</td>
</tr>
<tr>
<td>Edit Tier Name</td>
<td>Select a tier and click to change a tier name.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select a tier and click to delete a tier.</td>
</tr>
</tbody>
</table>

### 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.
5. 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.

6. 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.

7. 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**.
   
   d. 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.

8. To associate groups with this address book, click **Associate User 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.
d 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.

9 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.
   d 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.

10 Click OK.

**Editing an Address Book Settings**

Edit the fields in the Edit an Address Book dialog.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book Information</td>
<td></td>
</tr>
<tr>
<td>Address Book 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>Address Book Tiers</td>
<td></td>
</tr>
<tr>
<td>New Tier</td>
<td>Select where you want to add a tier and click to add a new tier to the address book.</td>
</tr>
<tr>
<td>Edit Tier Name</td>
<td>Select a tier and click to change a tier name.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select a tier and click to delete a tier.</td>
</tr>
</tbody>
</table>

**Assign Address Books to User 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 assign an address book to a group:

1 Go to User > User Groups.
2 Select the group you want to assign.
3 Click Edit .
4 In the Edit Local Group dialog, select address book you want from the Assign Address Book drop-down list.
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 from the More drop-down list.
   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 from the More drop-down list.
3. In the Default Address Book dialog, 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 from the More drop-down list.
4. In the Copy Address Book dialog, 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.
Direct Conference Templates

You use MCU conference templates when you schedule conferences to take place on an MCU that has been integrated with RealPresence Resource Manager system’s conferencing service.

Direct Conference Templates Overview

Direct templates are based on existing conference profiles that have been created on the MCU. You can choose to have the template automatically synchronized with its associated RealPresence Collaboration Server (RMX) profile by maintaining the routing name of the RealPresence Collaboration Server (RMX) profile or download the profile directly to the RealPresence Resource Manager system.

The RealPresence Resource Manager systems does not support scheduling conferences on third-party MCUs. Direct Conference template settings apply only to the RealPresence Collaboration Server (RMX) and MGC devices.

Users assigned the Administrator role can add Direct Conference Templates from any MCU that is integrated the RealPresence Resource Manager system’s conferencing services. They can also identify (by user role) which users have access to which Direct Conference Templates. Conference schedulers can then select from the different templates available to them to switch between different combinations of conference settings.

Direct conference templates do not display all available RealPresence Collaboration Server (RMX) settings. Nor or all conference settings defined in the template used by the RealPresence Resource Manager system when setting up a direct conference.

You create a direct conference templates in two ways:

- **Standalone Templates**: Download a conference profile from a managed MCU creating a “standalone” (free-standing) template independent of the profiles available on the system’s RealPresence Collaboration Servers, Polycom RealPresence Collaboration Server (RMX) systems, or Polycom MGC systems.
- **Linked Templates**: Link the template to a RealPresence Collaboration Server or RealPresence Collaboration Server (RMX) profile that exists on some or all of the MCUs.

Linked conference templates are not supported for Polycom MGC systems.

Conference templates for Pooled Conferences are created and managed on the Polycom RealPresence DMA system.
For more information about the RealPresence Collaboration Server (RMX) profile settings, see Polycom® RealPresence® Collaboration Server (RMX®) 1500/2000/4000 Administrator’s Guide.

**Standalone Templates**

Standalone templates defined in the RealPresence Resource Manager system free you from having to ensure that the exact same conference profiles exist on all the MCUs.

When it uses a standalone template for a conference, the system sends the specific properties to the MCU instead of pointing to one of its profiles.

**Considerations for Polycom MGC Systems**

Standalone or “downloaded” templates are the only ones allowed for use with Polycom MGC systems.

In addition, the RealPresence Resource Manager system does not support MGC templates that use the following dual stream settings: **Hi-Res Graphics or Live Video** setting.

**Linked Templates**

When you link a conference template to a template to a RealPresence Collaboration Server or RealPresence Collaboration Server (RMX) profile ensures that the template’s properties match the capabilities on the MCU selected for the conference.

This means that when you use a linked template for a conference, you must also select the specific MCU that contains the profile on which the template is linked.

When you link a template to a profile, it's up to you to ensure that the profile exists on the MCUs you want to use with that template and that its settings are the same on all of them.

If do not select the MCU from which the template is based, the scheduled conference will not launch.

As a best practice, when linking templates to MCU profiles, this will make it easier for conference schedulers to select the bridge that corresponds with the template.

This option is not supported for MGC conference profiles.

**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 particular 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 some settings of a standalone template.

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 localized their names into your language, edit the templates and enter new names for them.

When creating new direct conference 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).

- As a best practice, when linking templates to MCU profiles, give the template a name that includes the bridge name, this will make it easier for conference schedulers to select the bridge that corresponds with the template.

If your RealPresence Resource Manager system has areas enabled, be sure to give your area-specific names to your templates. This is particular helpful if you have schedulers who have been given permission to manage more than one area.

View the Direct Conference Templates List

You can view a list of added direct conference templates.

To view the MCU Conference Template list:

1. Go to Conference > Direct Conference Templates.
   The Direct Conference Templates list appears.
2. Select the template of interest from the list and click View.
   You can expand the settings description in the right pane of the screen.

Add a Direct Conference Template

When you add a template to the RealPresence Resource Manager from an MCU, you can use it for conferences you want to schedule. You can add conference templates from any MCU that is integrated with the RealPresence Resource Manager system's conferencing services.
To add a direct conference template:

1. Go to **Conference > Direct Conference Templates**.
2. On the **Direct Conference Templates** list, click **Add**.
3. In the **Select an MCU** dialog, choose an MCU from which to add a template and click **View Profile**.
4. In the **Select a Profile** dialog, choose an MCU conference profile to add as a template.
   - To link the template to its MCU profile, click **Use Routing Name**.
   - This option is not supported for MGC conference profiles.
   - To create a standalone template, click **Download Profile**.
5. In the **Add Direct Conference Template** dialog, you can customize the profile summary.
6. 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.

### Direct Conference Template Profile Settings

This table explains the direct conference template profile settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Template Name</td>
<td>Enter a unique and meaningful name for the template, which can be up to 50</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• RMX</td>
</tr>
<tr>
<td></td>
<td>• MGC</td>
</tr>
<tr>
<td></td>
<td>• RMX + MGC</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>
<tr>
<td>Dial Options</td>
<td>These settings apply only to video conferences. The video dial options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dial-In Only</strong> (all participants dial into the conference)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dial-Out Only</strong> (all participants are called by the system)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dial-In + Dial-Out</strong> (The person setting up the conference can specify which participants must dial into the conference and which participants are called by the system.)</td>
</tr>
</tbody>
</table>
Edit a Direct Conference Template

You can edit the profile of a direct conference template.

To edit a direct conference template:

1. Go to Conference > Direct Conference Templates.
2. On the Direct Conference Templates list, select the template of interest and click Edit.
3. Edit the Customized Profile Summary as needed.
4. Click OK.

Delete a Direct Conference Template

You can delete a direct conference template.

To delete a conference template:

1. Go to Conference > Direct Conference Templates.
2. On the Direct Conference Templates list, select a template and click Delete.
3. Click Yes to confirm the deletion.
RealPresence DMA Conference Templates

Anytime conferences and conferences scheduled to take place on a DMA Pool Order use conference templates that are created and managed in the RealPresence DMA system.

RealPresence DMA System Conference Templates for Multi-Tenancy

RealPresence DMA system conference templates cannot be assigned to a specific area. Area schedulers will be able to select from a list of all RealPresence 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 RealPresence DMA templates apply to his purview; for example, area_template.

Establishing Naming Conventions for RealPresence DMA System Templates

By default, all RealPresence DMA system conference templates are made available to conference schedulers who have permission to create pooled conferences and anytime conferences. To differentiate which RealPresence 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.

● A **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 email.

● 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.

### Configuring 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 RealPresence DMA conference template to use a RealPresence Collaboration Server profile that has Auto-Terminate enabled.

For more information about RealPresence Collaboration Server profiles and how to use an existing RealPresence Collaboration Server profile for a RealPresence DMA conference template, see *Polycom RealPresence DMA System Operations Guide*.

### Initiating Conference Dial-out

You can configure the RealPresence 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 RealPresence 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 do not select this check box, 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**.
Configuring Conference Settings

You can configure conference settings. Conference settings apply to conferences only. You can disable/enable time warnings, set whether the conference requires a passcode, automatically include the conference creator in conference, as well as enable overbooking of dial-in participants.

The settings you configure will be used for all conferences.

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 RealPresence Resource Manager system sends a message to video endpoints in a conference to warn the endpoint users that their conference is scheduled to end soon. The system sends the message 10 minutes, 5 minutes and 3 minutes before the conference is scheduled to end. To support this feature, the video endpoint system must be capable of receiving a system <strong>Send Message</strong> action. By default, <strong>Conference Time Warning</strong> is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This feature is not related to the MCU-based <strong>End Time Alert Tone</strong> feature.</td>
</tr>
<tr>
<td>Automatically Include</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>
<tr>
<td>Conference Owner (Scheduler) in New</td>
<td></td>
</tr>
<tr>
<td>Conferences</td>
<td></td>
</tr>
<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></td>
<td></td>
</tr>
</tbody>
</table>
### Specify Conference Settings

Navigate to the conference settings page to configure conference settings.

**To specify conference settings:**

1. Go to Conference > Conference Settings.
2. On the Conference Settings page, make the required selections.
3. Click Update.

### Disable Conference Time Warning

You can disable the warning that alerts users that their conference is ending.

**To disable the conference time warning:**

1. Go to Conference > Conference Settings.
2. In the Conference Time Warning section of the Conference Settings page, clear the Enabled check box.
3. Click Update.

### Conference and chairperson passcode length

Designate the required length of the system-generated conference and chairperson passcodes. The acceptable length for both of these passcodes is 4 to 16 characters. By default, the required length for both of these passcodes is set to 15 characters.

**Notes**

- 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 4 to 16 characters. By default, the required length for both of these passcodes is set to 15 characters.</td>
</tr>
<tr>
<td>Include the Web Suite URL in the notification email</td>
<td>Include the URL of the RealPresence Web Suite Experience Portal in the email notification for the meeting. Applicable for pooled and anytime conferences when the RealPresence DMA system is integrated with a RealPresence Web Suite.</td>
</tr>
<tr>
<td>Web Suite Server Address</td>
<td>The server address of the RealPresence Web Suite Experience Portal.</td>
</tr>
</tbody>
</table>
Automatically Include Conference Creator in Conference

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.

To automatically include the conference creator in the conference:

1. Go to Conference > Conference Settings.
2. Check the Automatically include conference creator (scheduler) in new conferences section of the Conference Settings check box.
3. Click Update.

Overbook 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.

This setting does not apply to guest participants. Guest participants can always be overbooked.

To allow schedulers to overbook dial-in participants:

1. Go to Conference > 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.

Set the Conference and Chairperson Passcode Length

You can designate the required length of the system-generated conference and chairperson passcodes. The acceptable length for both of these passcodes is 6 to 16 characters. By default, the required length for both of these passcodes is set to 15 characters.

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.

To set the passcode length:

1. Go to Conference > Conference Settings.
2 Mark the **Conference and chairperson passcode length** check box.

3 Click **Update**.

---

**Customizing Text to Email Notifications**

You can configure the system to send conference notification emails. The same text will be used for all conference notification email notifications. Within these emails, you can include customized text.

**Add Customized Text to Conference Email Notifications**

You can customize the text for your conference email notifications. This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.

**To add customized text to all conference E-mail notifications:**

1 Go to **Admin > Server Settings > E-mail**.

2 In the **The text entered below will be included with scheduling reminder E-mails** section of the **E-mail** page, type in the introductory text you want to appear at the start of all conferencing email notifications.

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 email notifications.

4 Click **Update**.

**Edit Customized Text in Email Notifications**

You can edit the customized text included in your conference notification emails.

**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 **The text entered below will be included with scheduling reminder E-mails** section of the **E-mail** page with the new text you want to appear at the start of all conferencing email 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 Email** section of the **E-mail** page with the new text you want to appear at the end of all conferencing email 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**.
Conference Scheduling

The RealPresence Resource Manager system can schedule and manage conferences, participants, and guest book.
Conference Scheduling Overview

The RealPresence Resource Manager system can schedule and monitor video conferences.

Log into the System

To log into the RealPresence Resource Manager system web interface, you need the IP address or host name of the RealPresence Resource Manager system server and your username, password, and domain. Generally, you get three opportunities to enter the correct password. After three failed attempts, the system returns an error message.

To log into the system:

1. Open a browser window and in the Address field enter the RealPresence Resource Manager system IP address or host name.
2. When the RealPresence Resource Manager system Log In screen appears, enter your Username and Password.
3. If necessary, select a different Language.
4. Click Login.

Conference Scheduler Roles

Users assigned a conference scheduling role can schedule 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>
</tbody>
</table>
## Conference Scheduling Overview

### Role | Supported Actions
--- | ---
Advanced Scheduler | Add a new conference  
  | Specify bridges and select templates for new conferences  
  | Copy a conference you created  
  | View details of a conference you created  
  | Edit some conference settings  
  | Delete a conference you created
Area Scheduler | Add a new conference  
  | Edit a future conference you created  
  | Copy a conference you created  
  | View details of a conference you created  
  | Delete a conference you created
Operator | Add a new conference  
  | Specify bridges and select templates for new conferences  
  | Copy any conference  
  | Edit any future conference  
  | Delete any future conference  
  | View any conference  
  | Manage any ongoing conference  
  | Terminate any ongoing conference
Area Operator | All area scheduler functions  
  | All advanced scheduler functions  
  | Manage any ongoing conference  
  | Terminate an ongoing conference

### Scheduling Participants

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.

Your RealPresence Resource Manager system configuration needs to include an NTP server to ensure successful scheduling. All resources of your video conferencing environment should be set to the same NTP server.

Scheduling Bridges and DMA Pool Orders

When you schedule a conference, you can select a single bridge or a RealPresence DMA pool order to host the conference, depending on the permissions that you have been given by the administrator.

**MCU Selection**

Users with the Advanced Scheduler or Operator role can select a MCU 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.

**Bridge Scheduling and Reassignment**

When you schedule a conference, the system automatically assigns the conference to a bridge unless a user with the default Advanced Scheduler or Operator 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 email message to all scheduled participants. This updated email includes a new dial-in number that dial-in participants must use to join the conference.
- 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.
- 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 email to notify the conference organizer of the failure.

**DMA Pool Orders**

Instead of selecting a bridge for your conference, you can select a RealPresence DMA pool order to manage your conference calls. This means that you do not need to track bridge availability or status of the conference resources manually. When you select a DMA pool order for your conference, your scheduled conference is hosted by the RealPresence DMA system. Using RealPresence DMA system defined priorities, the RealPresence DMA system can manage resource allocation between RealPresence...
Resource Manager system scheduled conferences and the RealPresence DMA-initiated ad hoc calls in real-time.

**Room ID Numbers**

When you schedule your conference on a DMA Pool Order, you can also create a room ID and dial-in number for participants to use. If you don’t specify a room ID, the RealPresence DMA system will create one and the RealPresence Resource Manager associates it with the scheduled conference.

You can also use an existing VMR number that has been created on the RealPresence DMA system, as long as the VMR is not already scheduled for the time you need it. When you use an existing RealPresence DMA VMR, you can view the VMR settings on the RealPresence DMA VMR as “scheduled” (including the time), but until the conference is started other settings will not display such as dial-out participants or additional settings. These settings only get sent to the RealPresence DMA when the conference starts.

**Limitations When Scheduling a Conference on a DMA Pool Order**

When scheduling your conference on a DMA pool order, you are limited by the following:

- You must use a modified dialing number when scheduling an ISDN dial-out participant. Use the Use Modified Dial Number check box when scheduling an ISDN dial-out participant.

**Conference Templates**

Users with Advanced Scheduler or Operator permissions can also specify a conference template to use. 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.

When using conference templates, keep in mind:

- 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 MCUs are stored in the RealPresence Resource Manager system, while conference templates for Pooled Conferences are defined in the RealPresence DMA system.

**Recurring Conferences**

When you schedule recurring conferences, the VMR associated with that recurring conference remains associated with that conference. You can use the VMR to schedule other meetings during its free time. For example, the VMR associated with a recurring conference scheduled at 9 a.m. to 10 a.m. on Mondays. You can still use this VMR to schedule other meetings from the 10 a.m. today to 9 a.m. tomorrow.
Anytime Conferences

Anytime conferences are scheduled RealPresence DMA 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 RealPresence Distributed Media Application™ (DMA) system.

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 Owner passcode is automatically generated and required to launch an Anytime conference.
- All Anytime conference participants receive an email indicating the VMR number. The owner will also receive the owner passcode needed to launch the conference. Optionally, you can also include a conference passcode that participants are required to enter.
- 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 not 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.
- You can terminate an anytime conference from the RealPresence Resource Manager UI. There is no impact on the VMR.
Conference Scheduling

You can schedule different types of conferences and add participants to the conferences.

Since Area Schedulers can perform both basic and advanced tasks, any references in this section to the Scheduler role also apply to the Area Scheduler role.

Schedule a Conference

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

When you schedule a conference, you specify the time, location and the list of participants. Optionally, you can also assign conference roles to participants such as lecturer or conference chairperson. Users with advanced scheduler or operator permission can also select a specific bridge and configure conference settings.

You can include individual participants, conference rooms or guests in conferences.

When scheduling conferences, be aware that the time displayed in the lower left corner of the RealPresence Resource Manager system is associated with the time clock of the local PC. Conferences are scheduled according to the time on the NTP server you configured to use.

To schedule a conference:

1. Go to Conference > Monitor View and click Add .

   Dial-in participants can be scheduled to dial into multiple conferences during the same time period; dial-out participants cannot.

2. Click Participant to view the Add Participants and Rooms dialog.

3. To add a participant:

   a. Select the Add Participants radio button.
   b. Click Filter and type all or part of the participant’s name (with wildcards) in either of the fields provided.
   c. Click Search.
   d. Select the participant you want from the search results.

4. To add a guest:
a In the **Add Participants and Rooms** dialog box, select the **Add Guest** radio button.
b Click **Filter** and type all or part of the participant’s name (with wildcards) in either of the fields provided.
c Click **Search**.
d Select the participant you want from the search results.

5 To add a room:
a In the **Add Participants and Rooms** dialog box, select the **Add Rooms** radio button.
b Select a site from the **Search for Rooms at a Site** drop-down list.
c Select a room from the list of rooms associated with the site you selected.

6 When finished adding participants, rooms, or guests, click **Close**.

7 Enter a new **Conference Name** or accept the system-generated name.

8 Use the **Bridge Selection** drop-down list to select a bridge or RealPresence DMA pool order for the conference.

You can only select a named bridge or pool order if you have the Advanced Scheduler or Operator role. If you do not have this role, select **Auto Bridge** or **Auto Pool Order**. RealPresence DMA pool orders are only available when your system is integrated with a RealPresence DMA system.

9 Select **Start Time**, **Duration**, and **End Time** for the conference.

10 If you want to make the conference recurring:
a Click **Recurrence** and in the **Appointment Recurrence** dialog, 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.
b Click **OK**.

11 Assign roles to participants. If the conference type and template support conference roles, you can associate conference roles with participants.
a Expand the **Role Settings** area.
b Use the drop-down lists to select **Lecturer**, **Video Chairperson**, or **Owner**. You must first add participants before assigning them a role.

12 To modify conference settings, expand the **Conference Settings** area.

Only users with the **Advanced Scheduler** or **Operator** role can modify conference settings.

13 Use advanced settings only if you are scheduling a conference directly on a bridge that is a Polycom MGC system. If you aren’t using a MGC system, you can ignore these settings.

14 Click **Schedule Conference**.

15 Optionally, send a notification e-mail to participants.
a To exit without sending an updated email message to your participants, click **Skip E-mail**.
b To send an updated email to your participants, copy additional people on the notification and/or add notes about the conference.
   Note that the **To**, **CC**, and **BCC** fields are ASCII only.
c Click **Send**.
## Related Topics

- Role Settings
- Conference Settings

## Role Settings

Configure role settings for a conference.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Required for an Anytime conference. The owner is the participant who dials into the conference and enters a passcode to start the conference.</td>
</tr>
<tr>
<td>Video Chairperson</td>
<td>Video Chairperson: 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>Chairperson Passcode</td>
<td>If you enable Enable Chairperson passcode, the system assigns a Chairperson Passcode and provides this password to the video chairperson in a separate email. When enabled for a conference, the chairperson must enter this password at his or the video endpoint to assume control of the conference. The length of the password is specified in the Conference and chairperson passcode length drop down list on the Conference Settings page.</td>
</tr>
<tr>
<td>Lecturer</td>
<td>Designates the participant as the main participant in the conference. If you designate a lecturer for a conference, that participant will not be muted if the video operator mutes all.</td>
</tr>
</tbody>
</table>

## Conference Settings

Configure conference settings.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Available for MCU or RealPresence DMA Pool Order Conference?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Type</td>
<td>Select <strong>Video</strong> or <strong>Audio Only</strong>. Video conferences can include audio participants. If you choose an audio-only conference, video participants can only participate on audio channels only and no video will be displayed.</td>
<td>MCU conferences only</td>
</tr>
<tr>
<td>Conference ID</td>
<td>By default, the system assigns a <strong>Conference ID</strong>. 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 same Conference ID cannot be used in conflicting time slots. For example, if you use the same Conference ID for a meeting (10:00 am - 11:00 am) and for another meeting (10:30 am - 11:30 am), the system will prompt you to enter a new Conference ID. Not available for Pooled Conferences.</td>
<td>MCU conferences only</td>
</tr>
<tr>
<td>Room ID</td>
<td>By default, the RealPresence DMA will assign VMR as a <strong>Room ID</strong>. You can leave this field empty.</td>
<td>RealPresence DMA Pool Order conferences only</td>
</tr>
<tr>
<td>Conference Passcode</td>
<td>By default, the system assigns an 15-digit <strong>Conference Passcode</strong> and provides this passcode to participants within the content of the conference notification email. You can change this passcode to another 4-digit through 16-digit number.</td>
<td>MCU conferences and RealPresence DMA Pool Order conferences.</td>
</tr>
<tr>
<td>Conference Template</td>
<td>The available conference templates are automatically filtered according to the <strong>Conference Mode</strong> you select and listed in alphabetical/numerical order. When choosing a template for a RealPresence DMA pool order conference, the template list is ordered by the priority that was defined for the template in the RealPresence DMA system.</td>
<td>MCU conferences and RealPresence DMA Pool Order conferences.</td>
</tr>
<tr>
<td>Billing Code</td>
<td>Billing code is listed if areas are enabled and billing codes have been assigned to the area. If areas are enabled and a billing code is not assigned, the call detail report will list the billing code as <strong>None</strong>.</td>
<td>MCU conferences and RealPresence DMA Pool Order conferences.</td>
</tr>
</tbody>
</table>
Configure Advanced Settings

Use advanced settings only if you are scheduling a conference directly on a bridge that is a Polycom MGC system. If you aren’t using a MGC system, you can ignore these settings.

Advanced settings include parameters related to dialing options and configuration of a Polycom MGC system which include content options, as well specific bit rates or modes to use.

To configure advanced settings:

1. Expand the Advance Settings area.
2. Complete the settings for the conference scheduled on a Polycom MGC system.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Available for MCU or RealPresence DMA Pool Order Conference?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Mode</td>
<td>All: Supports all conferences. Video Switching (VSW): Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen (the current speaker sees the previous speaker). If video switching mode is enabled: The minimum line rate available is 768 kbps (except for SD resolution, available only on v7 and newer Polycom MCUs with MPM+ or MPMx cards). All endpoints must connect at the same line rate, and those that don’t support the specified line rate are connected in voice-only mode. The video clarity, layout, and skins settings are not available. LPR is automatically turned off, but can be turned back on. Continuous Presence (CP): The MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities. Select this mode if scheduling only AVC endpoints. This is the only mode that supports the use of Polycom MCU profiles, third-party and legacy endpoints, and legacy RealPresence Collaboration Server (RMX) MCUs. SVC conferencing is only possible with Polycom MCUs and endpoints that support H.264 SVC. CP and SVC: The MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities. Select this CP and SVC if scheduling both AVC and SVC endpoints.</td>
<td>MCU Conferences only.</td>
</tr>
</tbody>
</table>
Conference Advanced Settings

Complete the settings for the conference scheduled on a Polycom MGC system.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial Options</td>
<td>You have three options:</td>
</tr>
<tr>
<td></td>
<td>• To create a conference for which the same dial-in information and a PIN code are assigned to all conference participants, use the <strong>Dial-In</strong> setting. This setting enables participants to dial in from an audio or video endpoint and connect to the same conference on the MCU.</td>
</tr>
<tr>
<td></td>
<td>• To dial out to all participants in the conference, use the <strong>Dial-Out</strong> setting.</td>
</tr>
<tr>
<td></td>
<td>• To allow participants both options, select <strong>Dial-In+Dial-Out</strong>.</td>
</tr>
<tr>
<td>Note</td>
<td>When you change a conference from <strong>Dial-In</strong> to <strong>Dial In+Dial Out</strong>, the selected resources remain set to <strong>Dial-In</strong>. You must change them manually. Not available for Pooled Conferences.</td>
</tr>
<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 Audio Only 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>
</tbody>
</table>
Schedule an Anytime Conference

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

If your RealPresence Resource Manager system is not integrated with a RealPresence DMA system, you cannot create an Anytime conference.

To schedule an Anytime conference:

1. Go to Conference > Monitor View and click Add.
2. Mark the Anytime check box which is to the right of the Bridge Selection drop-down list.
3. Click Participants to add participants to the conference.
   a. Select one of the following: Add Participants, or Add Rooms or Add Guest.
b Click Filter and type all or part of the participant or room name (with wildcards) in either of the fields provided. If searching for a room, use the Last Name or Room Name field.

c Click Search.

d Select the participant or room you want from the search results.

e To add a guest, select Add Guest, select a guest from the list and click Add Guest. You can also filter the list by clicking Filter and entering the last or the first name of the guest you want.

f Repeat these steps to add all required participants, rooms and guests and then click Close.

4 Enter a new Conference Name or accept the name that the system generated.

5 Use the Bridge Selection drop-down list to select a RealPresence DMA pool order for the conference.

6 Assign roles to participants. If the conference type and template support conference roles, you can associate conference roles with participants.

   a Expand the Roles Settings area.

   b Use the drop-down lists to select an Owner for the conference. You must first add participants before assigning them a role.

7 Configure conference settings.

   a Expand Conference Settings.

   b Enter a conference passcode.

8 (Optional) Enter a Room ID to use. If this field is empty, RealPresence DMA will assign a VMR number.

9 To save the conference details, click Save.

### Anytime Conference Role Settings

Configure the role settings for an anytime conference.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Required for an Anytime conference. The owner is the participant who dials into the conference and enters a passcode to start the conference.</td>
</tr>
<tr>
<td>Video Chairperson</td>
<td>Video Chairperson: 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>
</tbody>
</table>
Conference Scheduling

Scheduling a Point to Point Conference

Take the following into consideration when scheduling point to point calls:

- A point to point call only has two device participants.
- At least one endpoint should be a hardware such as Polycom HDX or RealPresence Group Series.
- Make sure the Always Use MCU property is galse in Customized Profile Summary of the selected conference template.
- Devices behind a firewall can be the caller side, but H.323 IP address call is not supported.
- The Bridge Selection should be Auto Bridge when scheduling a conference.

Copy an Existing Conference

You can copy an existing conference to be used as a template for a new conference.

By default, users with the scheduler roles see only their conferences in the All Conferences list, while users with the operator role see all the conferences on the system.

If you have configured areas, users with the operator role 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 Conference > Monitor View.
2. Select the conference of interest and click Clone .
3. If you used a template other than the default when you created the conference, re-select the template.
4. Make the required changes to the conference date, participants, rooms, or other settings.
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 email appears with a message indicating Conference Successfully Scheduled.
6. To exit without sending an updated email message to your participants, click Skip E-mail.
Edit a Future Conference

You can modify future conferences.

By default, users with the scheduler roles see only their conferences in the All Conferences list, while users with the operator role see all the conferences on the system.

If you have configured areas, users with the operator role see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To edit a conference:

1. Go to Conference > Monitor View.
2. Click Filter to display future conferences.
3. Select the conference of interest and click Edit.
4. If you select a recurring conference, a dialog 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.
5. Make the required changes to the conference date, participants, or other settings. For information on performing these tasks.
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 email appears with a message indicating Conference Successfully Scheduled.
7. To exit without sending an updated email message to your participants, click Skip Email.
8. To send an updated email to your participants, copy additional people on the notification and/or add notes about the conference.
   Note that the To, CC, and BCC fields are ASCII only.
9. Click Send.

The system sends the updated conference notification email message. The Conference > Monitor 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.

When you edit a participant’s settings, those settings are valid only for the current conference that you are scheduling.

To edit a participant’s settings:

1. Go to Conference > Monitor View.
2. Select a conference of interest and click Edit.
3. If you select a recurring conference, a dialog 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, click **Edit** beside a participant to open the **Edit Participant Settings** dialog.

5 In the **Edit Participant Settings** dialog, you can edit the participant settings as required.

6 When finished, click **OK**.

---

**Participant Settings**

Edit the participant settings in the **Edit Participant Settings** dialog.

<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>How will this participant/room/guest join the conference?</td>
<td>Select <strong>In Person</strong>, <strong>Audio Only</strong> or <strong>Use Video</strong>.</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>Select the Bit Rate at which the participant will join the conference. If you select Automatic, the participants bit rate will match the bit rate setting configured for the conference when it was scheduled.</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, SIP (SIP URI) or H.320. If no dial type is selected, it defaults to E.164.</td>
</tr>
</tbody>
</table>
| If H.323 is selected for Dial Type: | Number:  
| | • Completed automatically and is read-only when the user is not a guest.  
| | • Modify the number type if necessary (IP address, E.164, H.323, Annex-0)  
| | • Add an extension if needed.  |
| If SIP is selected for Dial Type: | • SIP URI: Completed automatically and is read-only when the user is not a guest.  |
| If ISDN is selected for Dial Type: | Enter the country code, area code, and phone number as necessary. Use a modified dial number if you need to dial a prefix or an outside line first.  |
| Encryption                    | Indicate if this participant will join the conference under encryption. Remember that the MCU that hosts the conference must be configured to support encryption for this setting to take effect. |
| 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. |
View Scheduling Information for a Conference

You can view scheduling information for a conference.

By default, users with the scheduler roles see only their conferences in the All Conferences list, while users with the operator role see all the conferences on the system.

If you have configured areas, users with the operator role 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 scheduled conference:

1. Go to Conference > Monitor View
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 detailed information of this conference is displayed on the right.

For details on the type of information that is provided, see Conference and Participant Details.
Managing Conferences and Participants

You can manage conferences and participants in the RealPresence Resource Manager system.

Working with Conferences

You can view ongoing, past, and future conferences. You can view them in a list view or calendar view. What you see depends on your user permissions. For example, if you have the view-only scheduler role, you cannot see the details of any conferences. Those with the operation role can view all conferences, including details.

View All Conferences

You can view both scheduled and ongoing conferences in the conference monitor view. You can toggle between a calendar and list view of all conferences.

When you view a conference, you can also view its status and any applicable alerts.

<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.</td>
</tr>
<tr>
<td>Completed Conference</td>
<td>A scheduled conference that occurred in the past.</td>
</tr>
<tr>
<td>Conference</td>
<td>A conference that is still ongoing.</td>
</tr>
</tbody>
</table>
| Alerts Conference  | The bridge on which the 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 does not apply to conferences scheduled on a RealPresence DMA Pool Order.                                     |
| Conference End Warning | The conference is ending. For example, the conference is in its last five minutes unless someone extends it. |

To view all conferences:

1. Go to Conference > Monitor View.

The All Conferences list displays a list of all conferences.
2. Select the 50, 100, or 200 from the Items per page list to display the conferences by page.

3. To view the list in calendar view, click Calendar View. The All Conferences page displays the conferences in a calendar view. Click Day, Week, or Month to change the calendar view.

4. To view the list in list view, click Calendar View again.

**Filter the Conference List**

You can filter the conference list to identify specific conferences you want to view. You must be in list view to filter the conference list. Filtering is not available in calendar view.

You can filter by a number of criteria including date, bridge, conference name and so on.

**To filter the conference list:**

1. Go to Conference > Monitor View. The All Conferences list displays a list of all conferences.

2. Click Filter to filter the All Conference list. The Filter dialog allows you to filter on the various criteria.

3. To filter by date:
   a. Click Today to filter on conferences happening today.
      Optionally, you can change the date to filter on conferences for a specific day.
   b. Click From and To to filter on conferences within a range of dates. Select From and/or To and fill in the dates in the following format: YYYY-MM-DD or use the calendar tool to select a date.

4. To filter by Anytime conferences:
   a. Mark the Anytime check box to see all Anytime conferences.
   b. Optionally, use the date filtering options in combination with the check box.

5. To filter by status:
   a. Click Status.
   b. Click the text box and select a status from the context menu. Available statuses include: All, Future, History, and Ongoing.
   c. Optionally, use the date filtering options in combination with the check box.

6. To filter by bridge:
   a. Click Bridge and fill in a bridge name in the text box.
   b. Optionally, use the date filtering options in combination with the check box.

7. To filter by dial in number:
   a. Click Dial in Number and enter a dial in number in the text box.

8. To filter by creator:
   a. Click Creator and enter first name or last name in the text box.

9. To filter by conference owner:
   a. Click Owner and fill in the owner’s name in the text box.
Managing Conferences and Participants

b Optionally, use the date filtering options in combination with the check box.

10 To filter by conference name:
   a Click **Conference Name** and fill in the conference name in the text box.
   b Optionally, use the date filtering options in combination with the check box.

11 To filter by endpoint name:
   a Click **Endpoint Name** and fill in the conference name in the text box.
   b Optionally, use the date filtering options in combination with the check box.

12 To filter by area:
   a Click **Area** and fill in the area name in the text box.
   b Optionally, use the date filtering options in combination with the check box.

13 When finished selecting criteria, press **Enter**.

Only 1000 results can be returned when there are over 1000 results.

14 Click **Reset** to clean all the conditions before you do another search.

**Delete a Conference**

You can delete scheduled or past conferences. You cannot delete active conferences.

**To delete a conference:**

1 Go to **Conference > Monitor View**.
2 If necessary, filter the **All Conferences** list to include the conference you want to delete.
3 Select the conference of interest and click **Delete**.
4 If you select a recurring conference, a dialog appears asking you if you want to delete just the conference you selected or all conferences in the series. Make the appropriate choice. You cannot deleted active conferences in the series.
5 Click **OK** to confirm the deletion.

The conference is deleted. For future conferences, the system emails the change to the conference owner and participants and releases the participant and room resources.

**Export a List of Scheduled Conferences**

Users with the Operator or Admin role can export a list of future conferences to a CSV file.

You can export a list of scheduled conferences. Ongoing or past conferences cannot be exported.

**To export a list of future conferences to a CSV file:**

1 Go to **Conference > Monitor View**.
2 In the **All Conferences** list, be sure you filter the conference list to include only scheduled conferences. You cannot export ongoing or past conferences.
3 Click **Download**.
Managing Active Conferences

Depending on your permissions, you can manage active conferences. For example, you can change the layout that participants see or add new participants.

RealPresence Immersive Studio systems display as expandable folders containing an icon for each of the codecs associated with the endpoint. You can only perform actions on the master codec. The master codec is indicated by name of the codec that ends with "_1".

Manage an Active Conference

You can manage an active conference. Users with the operator or advanced scheduler role can make changes to the conference, such as add new participants, terminate the conference and so on.

To manage an active conference:

1. Go to Conference > Monitor View.
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.
3. Use these actions under the Conference Actions drop-down list as needed:
   - Extend Duration: Extend the duration of an active conference.
   - Change Layout: For applicable endpoints. Change the default video layout for the conference display.
     - Switching. Indicates that the display changes each time the speaker changes, and everyone sees the current speaker.
     - Select a Frame Count, then select the specific layout for the frames.
       The available layouts are Continuous Presence settings.
   - Add Favorites: Add participants from one of your Favorites lists to the selected conference.
4. Use these under the Participant Actions drop-down list as needed. See Manage a Participant’s Endpoint During a Conference for details.

Related Topics

Manage a Participant’s Endpoint During a Conference
Participant List Settings

Participant List Settings

The Participants list displays these settings:
Write Conference Notes During a Conference

You can write conference notes when managing an ongoing conference.

To create a conference note:

1. Go to Conference > Monitor View.
2. Click Filter to filter the All Conference list to include the conference of interest.
3. From the list of All Conferences, select the conference of interest and click Manage.
4. Expand the Conference Notes pane on the far right of the screen.
5. Click inside the text box to type a note. If you type a note and then decide to undo your changes, click Escape to return to the original note.
6. Click Save.

The note becomes visible on any RealPresence Resource Manager browser session where other users are monitoring the same conference.
Add Additional Participants to an Active Conference

Users with the Operator role can add additional participants to an active conference.

To add participants from the local directory or enterprise directory:

1. Go to Conference > Monitor View.
2. Click Filter to filter the All Conference list to include the conference of interest.
3. From the list of All Conferences, select the conference of interest and click Manage.
4. Go to Conference Actions > Add Participant.
5. If necessary, edit the new participants’ settings.
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 Guests to an Active Conference

Users with the Operator role can add guests to an active conference.

If guests with the same dialstring and different extensions are added into a RealPresence DMA ongoing meeting, and then disconnected to the meeting. The guests may not reconnect to the meeting successfully. You need to remove the guests and add them back to the meeting manually.

To add participants from the Guest Book:

1. Go to Conference > Monitor View.
2. Click Filter to filter the All Conference list to include the conference of interest.
3. From the list of All Conferences, select the conference of interest and click Manage.
4. Go to Conference Actions > Add Participant.
   a. Click Filter and type all or part of the participant’s name (with wildcards) in either of the fields provided.
   b. Click Search.
   c. Select the participant you want from the search results. The guest’s name appears in the underlying New Conference Participants list.
5. To add new guest participants (participants not available from the local directory, enterprise directory, or Guest Book), do the following:
   a. Click the Add Guest radio button.
   b. Fill in the necessary information in the Add Guest dialog.
6. Click OK.
7. Click Close when you are finished adding guests.
   The added participants are listed in the New Conference Participants list at the bottom of the page.
8. To initiate the system dial out to new participants, select the participants 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**

You can add a room to an active conference.

**To add a room to an active conference:**

1. Go to Conference > Monitor View.
2. Click Filter to filter the All Conference list to include the conference you want to manage.
3. Select the conference of interest and click Manage.
4. From the Conference Actions list, click Add Room.
   a. Select a site from the Search for Rooms at a Site drop-down list.
   b. Select a room from the list of rooms associated with the site you selected.
      The conference room name appears in the underlying New Conference Participants list.
5. Click Close.
6. 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 a Participant’s Video During a Conference**

You can view a participant’s video during an ongoing conference. This is helpful to troubleshoot any video issues during the conference.

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

1. Go to Conference > Monitor View.
2. Click Filter to filter the All Conference list to include the conference you want to manage.
3. Select the conference of interest and click Manage.
4. Select a participant from the Participants list.
   The selected participant’s video appears in the Conference Image section of the interface.
5. 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 > Monitor View.
Managing Conferences and Participants

2  Click **Filter** to filter the **All Conference** list to include the conference you want to manage.
3  Select the conference of interest and click **Manage**.
4  From the **Conference Actions** list, click **Join Conference**.
   The **Join Conference** dialog appears.
5  If you have multiple endpoints, choose the endpoint to use to join the conference.
6  Click **Join Conference**.
   Your endpoint is added to the 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 > Monitor View**.
2  Click **Filter** to filter the **All Conference** list to include the conference you want to manage.
3  Select the conference of interest and click **Manage**.
4  From the **Conference Actions** list, click **Add Favorites**.
5  From the **Favorites List**, expand the list of interest.
   The names of the participants in the list is displayed.
6  Select the participant of interest from the list.
   The participant’s name appears in the underlying **New Conference Participants** list.
7  Repeat steps 5 and 6 to add all participants from **Favorites List** and then click **Close**.
8  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.

**Terminate an Active Conference**

You can terminate an active conference.

To terminate an active conference:

1  Go to **Conference > Monitor View**.
2  Click **Filter** to filter the **All Conferences** list to include the conference you want to terminate.
3  Select the conference of interest and click **Terminate**.
4  Click **Terminate** to confirm the termination.
Managing Participants within an Active Conference

When monitoring a conference, you can manage the participants within the conference. You can manage their endpoints, and view the technical details of their connection.

Add or 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. Click Filter to filter the All Conference list to include the conference you want to manage.
3. Select the conference of interest and click Manage.
4. From the Participants list, select the participant of interest.
5. From the Participant Actions menu, click Save as Favorite.
   The names of the participants in the list is displayed.
6. From the Save as Favorite Participant dialog, select the Favorite List to which to save the participant and click OK.

Manage a Participant’s Endpoint During a Conference

You can manage a participant’s endpoint during a conference.

When using the commands on the manage page, these context-sensitive commands only appear when the participant’s endpoint supports the action, and the commands work for rooms on the participant list as well.

To manage a participant’s endpoint:

1. Go to Conference > Monitor View.
2. Click Filter to filter the All Conferences list to include the conference you want to manage.
3. Select the conference of interest and click Manage.
4. Select a participant to manage from the Participants list.
5. From the Participants Actions list, select View.
6. From the View Participants Details dialog, choose a manage option from the right section of the dialog.

Managing Participant Settings

The table explains the options on the View Participants Details dialog.
Managing Conferences and Participants

View a Participant’s Details During a Conference

You can view details for a participant’s endpoint while the participant is in conference.

RealPresence Immersive Studio systems display as expandable folders containing an icon for each of the codecs associated with the endpoint. You can only perform actions on the master codec. The master codec is indicated by name of the codec that ends with “_1”.

To view a participant’s endpoint details:

1. Go to **Conference > Monitor View**.
2. Click **Filter** to filter the **All Conferences** list to include the conference you want to manage.
3. Select the conference of interest and click **Manage**.
4. From the **Participants** list, select a participant to view.
5. Click **Participant Actions > View**.
6. Double-click on the participant of interest.

The **View Participant Details** dialog 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**.
7 To view additional participant details, change the selection in the **Call Properties** drop-down menu.
- Select **Device** to view the participant device related details.
- Select **Call Details** to view the participant call related 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.

**Related Topics**

Manage a Participant’s Endpoint During a Conference
Participant Device Related Details
Participant Call Related Details

**Participant Device Related Details**
The table explains the participant device related 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: PVX, MGC, 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, email, Party Number, and Unknown.</td>
</tr>
<tr>
<td>Alias Value</td>
<td>Value for the alias type shown.</td>
</tr>
</tbody>
</table>

**Participant Call Related Details**
The table explains the participant call related details.
<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>The cause code showing how the call ended.</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>
Managing the Guest Book and Favorites Lists

The RealPresence Resource Manager system provides two ways that you can customize and expand the user directories. The system has a Guest Book and a Favorites List.

Managing the Guest Book

Users with the schedulers, operator, or administrator role have access to the Guest Book. The Guest Book provides a way to store conference participants that aren’t managed by the RealPresence Resource Manager system.

The Guest Book is a local system directory that includes guest participants who were either explicitly added to the Guest Book or saved to the Guest Book while being added as conference participants.

Guest book entries are static and are not imported through the dynamically updated enterprise directory nor included in the system Global Address Book. The Guest Book is limited to 500 entries.

Users with the schedulers, operator, or administrator role have access to the Guest Book. The Guest Book provides a way to store conference participants that aren’t managed by the RealPresence Resource Manager system.

View the Guest Book

By default, both system and area schedulers, operator, and administrators have access to the Guest Book. When areas are enabled for your system, you can view only those guests who have been assigned to an area that you manage. If you can manage more than one area, you can view users from all areas that you manage.

To view the Guest Book:

1. Go to User > Guest Book.
2. Click Filter to filter the guest book by entering the first or the last name of the guest you want to find.
3. Click Search to get a filtered list. Or click Reset to clear your inputs. The Guest Book pages includes a list of guest book entries.

Guest Book Entries

The Guest Book pages includes a list of guest book entries that includes these fields.
Managing the Guest Book and Favorites Lists

Add a Guest to the System Guest Book

You can add a guest to the guest book.

You can add as many as 500 guests, but each guest must be unique. The RealPresence Resource Manager validates each guest for a unique H.323 ID, E.164 number, IP address, and so on. The RealPresence Resource Manager verifies that the guest does not already exist in the guest book or as a user-associated endpoint.

You can also add a new guest to the guest book when you are scheduling a conference.

To add a guest to the system Guest Book:

1. Go to User > Guest Book and click Add .
2. Configure the Guest Information section of the Add New Guest dialog.
3. If the guest has an H.323 (IP) endpoint, configure the H.323 (IP) settings.
4. If the guest has a SIP (IP) endpoint, configure SIP (IP) settings.
5. If the guest has an H.320 (ISDN) endpoint, configure the H.320 (ISDN) settings.
6. Click OK.

Related Topics

Guest Information
H.323 (IP) Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Name</td>
<td>The guest’s first and last name.</td>
</tr>
<tr>
<td>E-mail</td>
<td>The guest’s email address. The system validates the email structure only.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the guest’s endpoint system. This is a free-form entry field that the system does not validate.</td>
</tr>
<tr>
<td>Number</td>
<td>(Optional) The ISDN phone number for the user. This number is constructed from the Country code + Area/City code + phone number or entered as the modified dial number.</td>
</tr>
<tr>
<td>Join Mode</td>
<td>Indicates whether the guest will use an audio endpoint or video endpoint to join conferences.</td>
</tr>
<tr>
<td>Dial Options</td>
<td>Indicates whether the guest will dial into conferences or that the system 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) endpoint.</td>
</tr>
<tr>
<td>Selected Area</td>
<td>This field is available when areas are enabled and the user can manage more than one area.</td>
</tr>
</tbody>
</table>
Managing the Guest Book and Favorites Lists

SIP (IP) Settings
H.320 (ISDN) Settings

Guest Information
The table explains the Guest Information section of the Add New Guest dialog.

<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 email address. The system only validates the structure of the</td>
</tr>
<tr>
<td></td>
<td>email address.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the guest's endpoint system. This is a free-form field that</td>
</tr>
<tr>
<td></td>
<td>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),</td>
</tr>
<tr>
<td></td>
<td>or H.320 (ISDN). This selection will determine what other sections of the</td>
</tr>
<tr>
<td></td>
<td>Add New Guest dialog 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</td>
</tr>
<tr>
<td></td>
<td>each endpoint.</td>
</tr>
<tr>
<td>Dial Options</td>
<td>Specify whether the guest will dial into conferences, or require that the</td>
</tr>
<tr>
<td></td>
<td>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>
<tr>
<td>Assigned Area</td>
<td>This field is available when areas are enabled and the user can manage more</td>
</tr>
<tr>
<td></td>
<td>than one area.</td>
</tr>
</tbody>
</table>

H.323 (IP) Settings
The table explains the H.323 (IP) settings for H.323 endpoint.
Managing the Guest Book and Favorites Lists

### SIP (IP) Settings
The table explains the SIP (IP) settings for SIP endpoint.

<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. |

### H.320 (ISDN) Settings
The table explains the H.320 (ISDN) settings for H.320 (ISDN) endpoint.

<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 <strong>Use Modified Dial Number</strong> is selected.) The country to which the system will dial out to the guest. Click <strong>Select</strong> to view a list of country codes.</td>
</tr>
</tbody>
</table>
Edit a Guest in the Guest Book

You can edit information associated with a guest in the guest book.

If you edit a guest that is already scheduled for a future conference or participating in an ongoing conference, the changes you make will not be reflected in the conference.

To edit a guest in the system Guest Book:

1. Go to User > Guest Book and select the guest of interest.
2. Click Edit .
3. Change the Guest Information section and endpoint information sections of the Add New Guest dialog, as needed.
4. Click OK.

Delete a Guest from the Guest Book

You can delete a guest from the 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 . Click OK to confirm the deletion.

Managing Favorites

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.

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

You can create a new Favorites list.
Managing the Guest Book and Favorites Lists

To add a Favorites list:

1. Go to Conference > Favorites.
2. On the Favorites page, click Add +.
3. Enter a unique name for the Favorites List Name.
4. Enter a description.
5. Click Filter 📡 and enter all or part of the person’s last name or first name in the Search Available Members field 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.
- The search results only include users associated with endpoints.

6. Select the user(s) of interest from the list and move them to the Favorite List Members column.
7. Repeat step 5 and 6 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

You can edit a Favorites list. You can rename it or remove or add users to the list.

To edit a Favorites list:

1. Go to Conference > Favorites.
2. Select the Favorites list of interest and click Edit ✏.
3. In the Edit Favorites List dialog, 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

You can delete a Favorites list. When you delete a Favorites list, the users remain in the system but are not associated with the deleted Favorites list.

To delete a Favorites list:

1. Go to Conference > Favorites.
2. Select the Favorites list of interest and click Delete ✗.
3. Click OK to confirm the deletion.

The list is deleted from the system.
Conference and Participant Details

When scheduling and configuring a conference, see the conference and participant detail fields.

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.</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</td>
</tr>
<tr>
<td></td>
<td>between the local time and the standard time.</td>
</tr>
<tr>
<td></td>
<td>For an unscheduled conference, the date and time the conference started.</td>
</tr>
<tr>
<td>Duration</td>
<td>For a scheduled conference, how long the conference is scheduled to last.</td>
</tr>
<tr>
<td></td>
<td>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>
<tr>
<td>Type</td>
<td>The type of conference. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Audio</td>
</tr>
<tr>
<td></td>
<td>• Audio-Video</td>
</tr>
<tr>
<td>Status</td>
<td>The state of the conference. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Alerts</td>
</tr>
<tr>
<td></td>
<td>• Declined</td>
</tr>
<tr>
<td></td>
<td>• Finished</td>
</tr>
<tr>
<td></td>
<td>• Future</td>
</tr>
<tr>
<td>Recurring</td>
<td>Whether or not the conference was scheduled as a recurring conference.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connection</td>
<td>Connection information about the conference. Possible values include: Multipoint, Point To Point, Gateway, Embedded Multipoint</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>The rate (in kbps) at which to transfer the conference audio or video data.</td>
</tr>
<tr>
<td>Conf Monitoring ID</td>
<td>System-assigned ID used for troubleshooting.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Describes the media type used for the conference.</td>
</tr>
<tr>
<td>Video Session Type</td>
<td>Type of video session: VSW (Video Switching), CP (Continuous Presence), SVC (Scalable Video Coding) only CP and SVC</td>
</tr>
<tr>
<td>Video Layout</td>
<td>The video layout for the conference. For more information about layouts, see your MCU documentation. 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</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Video Format</td>
<td>For a conference hosted on an MCU, the video format of the conference data stream. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Automatic</td>
</tr>
<tr>
<td></td>
<td>• CIF</td>
</tr>
<tr>
<td></td>
<td>• QCIF</td>
</tr>
<tr>
<td></td>
<td>• 4CIF</td>
</tr>
<tr>
<td></td>
<td>• 16CIF</td>
</tr>
<tr>
<td>Video Protocol</td>
<td>For a conference hosted on an MCU, the video protocol of the conference data stream. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Auto</td>
</tr>
<tr>
<td></td>
<td>• H.261</td>
</tr>
<tr>
<td>Audio Algorithm</td>
<td>For a conference hosted on an MCU, the audio compression ratio of the conference data stream. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• AUTO</td>
</tr>
<tr>
<td></td>
<td>• G.711</td>
</tr>
<tr>
<td>Conference Area</td>
<td>Area or areas assigned to the selected conference owner.</td>
</tr>
<tr>
<td>Participant Areas</td>
<td>List of areas to which participants belong.</td>
</tr>
</tbody>
</table>

### 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></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The RealPresence Collaboration Server (RMX) 1000 system does not support the <strong>Chairperson</strong> 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>Dial-in #</td>
<td>The number that can be used by participant not explicitly invited to the scheduled 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>Lecture Mode</td>
<td>The type of <strong>Lecture Mode</strong>, if any, that was selected when the conference was created. Possible values are None, Lecture, and Presentation.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The RealPresence Collaboration Server (RMX) 1000 system does not support <strong>Lecture Mode</strong>.</td>
</tr>
<tr>
<td>Lecturer</td>
<td>The name of the lecturer. Not applicable when <strong>Lecture Mode</strong> 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></td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>- Duo Video</td>
</tr>
<tr>
<td></td>
<td>- Unknown</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 - 6.4</td>
</tr>
<tr>
<td></td>
<td>- MLP - 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>
### Participants

When you view a particular conference, the list of participants identifies users, rooms, and guests invited to participate. When viewing a conference, the list of participants identifies participants on a call.

<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>
</tbody>
</table>

---

When viewing a particular conference, the list of participants identifies users, rooms, and guests invited to participate. When viewing a conference, the list of participants identifies participants on a call.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU Name</td>
<td>If the conference is hosted on an MCU, shows 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 RealPresence Resource Manager system enables entry queues on a per MGC basis and all conferences on an entry queue enabled MGC 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>Conference on Port</td>
<td>(MGC only) Indicates whether or not the MGC is set to Conference on Port, which conserves bandwidth and ports. In this case, all participants are on a single video port and use the same connection speed and video format.</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>
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>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>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>
Endpoint Management

The RealPresence Resource Manager system can manage, monitor, and provision Polycom and third-party endpoints.
Managing Endpoints and Peripherals

You can manage and monitor endpoints and peripherals using the RealPresence Resource Manager system.

Endpoint Management

Endpoint management eliminates the need to configure each endpoint individually through the hand-held remote or the endpoint’s web interface. It also helps you easily enforce network, group, and system policies for each device.

Endpoint management consists of two aspects of remotely configuring endpoints: updating software and provisioning settings.

Scheduled Management of Video Endpoints (Polycom and Third-Party)

Scheduled management enables you to push software updates and provisioning profiles to endpoints at intervals that you define.

Scheduled 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.

Password Requirements for Scheduled Management

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.

**Dynamic Management of Video Endpoints (Polycom Only)**

Dynamic management enables the endpoint to poll the RealPresence Resource Manager automatically to get provisioning updates (configuration settings) and software updates based on policies you define. The administrator can use a rule-based system to apply dynamic provisioning profiles. An administrator can create multiple rules and associate a profile with more than one rule at a time. A provisioning rule consists of one or more conditions that must be met before the dynamic provisioning profile can be applied. Dynamic management is client-to-server over HTTPS which makes it more secure and firewall-friendly.

Dynamic management is available:

- Only for Polycom endpoints.
- When Polycom endpoints are able to automatically discover the RealPresence Resource Manager. This means you need to add the DNS service record (SRV record) for the RealPresence Resource Manager system.

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 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.

**Presence Service for Dynamically-Managed Endpoints**

The RealPresence Resource Manager system also provides a presence service to dynamically-managed endpoints. The presence service maintains online status information for the users of dynamically-managed endpoints. The presence service enables 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 an 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 reaching the user.

The RealPresence Resource Manager supports presence services for all dynamically-managed Polycom endpoints with the exception of RealPresence Mobile. RealPresence Desktop clients managed by the RealPresence Resource Manager can receive offline messages.

Understanding Dynamic Endpoint Management

**Managing UCS Phones**

The RealPresence Resource Manager system can be used as a central provisioning server for supported conference phones when your deployment uses a Cisco Unified Communication Manager as the voice call manager.
This allows you to use phone provisioning profiles to apply a single set of parameters and settings to all of the phones in your deployment. The use of phone provisioning profiles can reduce the time it takes to deploy new phones and configuration changes to existing phones.

You can also automatically send software updates.

**Managing Phones**

**Management of H.323 Endpoints Synchronized from a RealPresence DMA System**

H.323 endpoints that register with the RealPresence DMA system’s gatekeeper automatically display in a RealPresence Resource Manager system that has been configured with a RealPresence DMA system. This allows you to track the endpoints registered to the RealPresence DMA system. Once they are synchronized to the RealPresence Resource Manager, you can associate users with them if you want to manage the H.323 endpoints (provision or update) or schedule them into conferences.

Each synchronized DMA-registered endpoint consumes a device license in the RealPresence Resource Manager system.

For complete information about how to manage H.323 endpoints that are synchronized from a RealPresence DMA system, see *Working with Endpoints Synchronized from a RealPresence DMA System*.

**Calendar Connector**

The following Polycom endpoints can display a meeting calendar when associated with a Microsoft Exchange user: RealPresence Group Series systems, Polycom HDX systems, RealPresence Desktop video collaboration softwares, and RealPresence Mobile applications.

This means that in general, users of these systems can join meetings by clicking in the calendar display instead of manually dialing into the conference.

For an endpoint user to be able to use the feature, you must configure the RealPresence Resource Manager system to be a connector for the Microsoft Exchange Server. When you do this, the Calendar Connector service ensures that the right meeting information is routed to the endpoint’s calendar.

The Calendar Connector interprets the meeting invitations sent to the user via Microsoft Exchange and ensures that the endpoint can correctly dial a meeting directly from its calendar interface. It modifies the dial string within the invitation to ensure it is valid.

As an administrator, you must do the following:

- Configure the RealPresence Resource Manager to be a Calendar Connector
  This enables the RealPresence Resource Manager to act as a proxy service for your Exchange Server.

- Set up connector rules that scan emails for call information to insert into a user-associated Polycom endpoint’s calendar.

- Provision the user-associated endpoint to use the RealPresence Resource Manager system as its Exchange Server IP address.

  OR

- Manually configure the endpoint to use the RealPresence Resource Manager system’s IP address for its Microsoft Exchange server.
Configure the Calendar Connector

If you manage a supported Polycom endpoint (RealPresence Group Series, HDX, RealPresence Desktop or RealPresence Mobile), you can use the Calendar Connector feature to ensure that those endpoint users can click to join meetings directly from the endpoint’s calendar interface.

The Calendar Connector allows you to use the RealPresence Resource Manager system as a connector for your Microsoft Exchange Server. It interprets the meeting invitations sent to the user’s endpoint via Microsoft Exchange and ensures that the endpoint can correctly dial a meeting directly from its calendar interface. It modifies the dial string within the invitation to ensure it is valid.

You must have Admin permissions to configure the Calendar Connector.

To configure the Calendar Connector:

1. Go to Endpoint > Calendar Connector.
2. Click Add .
3. In the Add a Connector dialog, select the General section to enter a server type and server information.
   - Type: Only Exchange is supported for this release. Yahoo, Google, Office365, and Office365(China) are not officially supported in this release.
   - Server: Enter the server details for the calendar server type you selected.
   - Options: Configure the max concurrent sessions allowed.
4. You need to add at least one Connector Rule before you click OK. For more information about Connector Rule, see Add a Connector Rule.

Add a Connector Rule

You can create rules to help the connector find dial string information the meeting invitation to ensure it is in the user’s calendar.

Connector rules are regular expressions that interpret meeting invite fields to retrieve VMR information for the calendar. For connector rules to work effectively, your users must schedule meetings with consistent conference room identifiers that can be read by the rules you create.

For example, when scheduling a meeting with Microsoft Outlook, a user can specify the meeting location as below:

Location: Conference Room Marconi; VMR: 734567
or
Location: Conference Room Marconi; Bridge: 734567

In this case, the following match string would extract the VMR number 735467 from the meeting invite contents:

?:^|Bridge:\|VMR:\|vmr:\")s*(\d+)$

To create a connector rule:

1. Go to Endpoints > Calendar Connector.
2. Select a connector to edit and click Edit .
3. In the **Edit a Connector** dialog, select **Rules** to view the rule information.

4. Click **Add** +.

5. In the **Add a Rule** dialog, enter the rule parameters you want to use.

6. Click **OK**.

**Connector Rule Parameters**

The table explains the connector rule parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match For</td>
<td>Choose either <strong>Lync Meeting Invitation</strong> or <strong>Standard Meeting Invitation</strong>.</td>
</tr>
<tr>
<td>Invitation Field</td>
<td>Choose the meeting invitation field where you expect the VMR information to be. If you selected <strong>Lync Meeting Invitation</strong>, this field is grayed out.</td>
</tr>
<tr>
<td>Match String of Domain (Lync Invitation only)</td>
<td>Enter the Lync or Skype for Business domain name. For example, pctc-prmqa1.com</td>
</tr>
<tr>
<td>Match String of VMR Number (Standard Meeting Invitation only)</td>
<td>Enter a regular expression to use to detect the VMR number.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Enter a prefix to append to the beginning of the VMR number.</td>
</tr>
<tr>
<td>Suffix</td>
<td>Enter a suffix to append to the end of the VMR number.</td>
</tr>
<tr>
<td>Routing Method</td>
<td>Use the default setting (tel).</td>
</tr>
</tbody>
</table>

**Add a Filter for Unaccepted Meetings**

You can add a filter to the endpoint calendar so that meetings that are not accepted are not displayed.

**To add a filter:**

1. Go to **Endpoint > Calendar Connector**.
2. Select a connector to edit and click **Edit** /.
3. In the **Edit a Connector** dialog, select **Filters** to view the filter information.
4. Enter **(Busy)** in the **Match** field. This will create a filter that displays only meetings that are accepted (or busy).
5. Click **Save**.

**Dynamically Provision Calendar Connector Information**

If you have configured a Calendar Connector, you can dynamically provision Group and HDX systems with this information by dynamically provisioning the endpoints with the RealPresence Resource Manager FQDN instead of the Exchange Server address in a Network Config profile.

The Calendar Connector feature is only for supported Polycom endpoints: RealPresence Group, HDX systems, RealPresence Desktop, and RealPresence Mobile systems.
Managing Endpoints

From the Monitor View page, you can view the endpoint status, customize endpoint list, edit endpoints, reboot endpoints, and manage the endpoint associations.

View the Endpoint List

You can view all the provisioned endpoints listed in the Monitor View screen.

To view endpoints:

» Go to Endpoint > Monitor View.

Endpoint Information

The following table explains the endpoint information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</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>• Licensed</td>
</tr>
<tr>
<td></td>
<td>• In a call</td>
</tr>
<tr>
<td></td>
<td>• Gatekeeper/SIP/Cloud Service Registered</td>
</tr>
<tr>
<td></td>
<td>• Gatekeeper/SIP/Cloud Service/Signaling Unregistered</td>
</tr>
<tr>
<td></td>
<td>• Registration Status Unknown/Not Applicable</td>
</tr>
<tr>
<td></td>
<td>• Endpoints behind Firewall</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td></td>
<td>• Warning</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>Note:</td>
<td>If a phone crashes while in a call, the phone status may not update after it</td>
</tr>
<tr>
<td></td>
<td>reconnects to the RealPresence Resource Manager system. When the RealPresence</td>
</tr>
<tr>
<td></td>
<td>Resource Manager system gets a new call status from the phone or detects that</td>
</tr>
<tr>
<td></td>
<td>the phone is offline, the system updates the phone’s call status.</td>
</tr>
<tr>
<td>Mode</td>
<td>The management mode for the endpoint. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Non-dynamically Managed Endpoints</td>
</tr>
<tr>
<td></td>
<td>• Dynamically Managed endpoints</td>
</tr>
<tr>
<td></td>
<td>• Synced RealPresence DMA Endpoints</td>
</tr>
<tr>
<td></td>
<td>• Synced CUCM Phones</td>
</tr>
<tr>
<td></td>
<td>• Auto-added Phones</td>
</tr>
<tr>
<td></td>
<td>• Manually Added Phones</td>
</tr>
<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 Supported Endpoints and</td>
</tr>
<tr>
<td></td>
<td>Peripherals.</td>
</tr>
</tbody>
</table>
Customize the Endpoint List

You can filter the endpoint list and customize the columns that appear on the screen.

To customize the endpoint list:

1. Navigate to Endpoint > Monitor View.
2. Click Filter to filter the endpoint list using the conditions.
3. Click Reset if you want to do another search.
4. Press Enter to do the search.
5. Enter a key word in the Search field beside filter Filter to search the key word among the filter results. The key word search does not work for Area.
6. Click Columns to customize the columns that appear on the screen. By default, the MAC Address, Endpoint Group, and Software Version is not displayed.
7. To hide a column, cancel the check box next to the column that you wish to hide.
8. To display a column, mark the check box next to the column that you want displayed.

Endpoint Filter Conditions

The table explains the endpoint filter conditions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Filters the list by type.</td>
</tr>
<tr>
<td>Model</td>
<td>Filters the list by model name entered.</td>
</tr>
</tbody>
</table>
### Managing Endpoints and Peripherals

**View Endpoint Details**

You can view more details about an endpoint listed in the **Monitor View** screen.

#### To view detailed information about a managed endpoint:

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

   Depending on the selected endpoint type, you may see different information.

   **Device Status**, **Device Alerts**, **Software Update Details**, **Provisioning**, and **Details** are only available for video endpoints.

   **Endpoint Files** and **Configuration Profile Association** are only available for phones.
## Endpoint Details

The table explains the endpoint details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Summary</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Name          | The name of the endpoint.  
• Endpoint names must be unique.  
• The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid.  
• The system name might be different than the H.323 ID. |
| Type          | The type of endpoint. For valid types, see Supported Endpoints and Peripherals. |
| ID            | The system-generated ID for the device.                                         |
| Owner         | The person to whom the endpoint is assigned.                                   |
| IP Address    | The assigned IP address of the endpoint.                                       |
| VLAN ID       | (Phone Only) Virtual Bridged LAN ID                                            |
| Site          | The network site for the endpoint. By default, endpoints are added to the Primary Site.  
**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. |
| Software Version | The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed. |
| Serial Number | The serial number (ASCII only) of the endpoint. The endpoint provides the serial number if it registered successfully or is managed. |
| MAC Address   | (Phone Only) The MAC address of the endpoint.                                  |
| 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:  
&lt;username&gt;@host(domain or IP):Port |
| 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. |
| ISDN Video Number | (Video Endpoint Only) 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. |
| Available to Schedule | (Video Endpoint Only) It shows if this endpoint is available for conference scheduling. |
### Field | Description
--- | ---
Monitoring Level | (Video Endpoint Only) The monitoring level for the device. Possible values include:  
- **Standard.** This device is monitored.  
- **VIP.** This device is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.

Supported Protocols | (Video Endpoint Only) The communications protocols that the endpoint can support. Possible values include:  
- **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based H.323 networks.  
- **IP (SIP)** - A standard that defines the protocols used for multimedia communications on SIP networks.  
- **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.  
For endpoints with the type **Unknown**, select **H.323**. The endpoint automatically provides the protocols if it registered successfully or is managed.

Capabilities Enabled | (Video Endpoint Only) Capabilities enabled on this endpoint. Options are:  
- **MCU** - The endpoint can act as a control unit for multipoint conferences.  
- **Gateway** - The endpoint can act as a gateway for call management. The MCU provides the capability if it registered successfully or is managed.

Aliases | (Video Endpoint Only) 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, email, 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.  
**Note**  
- The following **Alias Values** are ASCII only: **H323 ID**, **URL**, **Transport Address**, and **Unknown**.

User | (Phone) The user ID mapped to the phone's SIP URI.

Uptime | (Phone) The time of the endpoint has been working and available.

Last Restart Time | (Phone) Endpoint’s last reboot or restart time.

Last Touch Time | (Phone) The last time that the endpoint connects to the RealPresence Resource Manager system.

Last Provisioning Time | (Phone) The last time that the RealPresence Resource Manager system sends provisioning configurations to the endpoint.

**Device Status (Video Endpoint Only)**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatekeeper Registration</td>
<td>The status of the device’s registration with the gatekeeper service. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Registered</td>
</tr>
<tr>
<td></td>
<td>• Unregistered</td>
</tr>
<tr>
<td>Directory Registration</td>
<td>The status of the device’s registration with the Global Directory Service. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Registered</td>
</tr>
<tr>
<td></td>
<td>• Unregistered</td>
</tr>
<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 RealPresence Resource Manager system is dynamically 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>SIP Server Address</td>
<td>The IP address of the SIP server.</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></td>
<td>This field is blank for the following device types: RMX, GW/MCU, Other, and TANDBERG.</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 device types: RMX, GW/MCU, Other, and TANDBERG.</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 RealPresence 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 RealPresence 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: RMX, GW/MCU, Other, and TANDBERG.</td>
</tr>
</tbody>
</table>
### Device ISDN Type
The ISDN network interface type installed in the device. Possible values include:
- ISDN QUAD_BRI
- ISDN PRI_T1
- ISDN BRI
- ISDN UNKNOWN
This field is blank for the following device types: RMX, GW/MCU, Other, and TANDBERG.

### Call Info

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Type</td>
<td>(Video Endpoint Only) Type of call, such as H.323, SIP, ISDN, or POTS.</td>
</tr>
</tbody>
</table>
| Video Protocol         | (Video Endpoint Only) The video connection protocol, both transmission (Tx) and reception (Rx), the endpoint 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           | (Video Endpoint Only) The video format, both transmission (Tx) and reception (Rx), the endpoint is using. |
| Audio Protocol         | (Video Endpoint Only) The audio connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include:  
  - G.711  
  - G.722  
  - G.728 |
| Far Site Name          | 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 ' | ', for example 'ISDN-CO1-7-1 | Vsfx-9-1'. |
| Far Site Number        | 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. |
| Cause Code             | (Video Endpoint Only) The cause code showing how the call ended. |
| Encryption             | (Video Endpoint Only) The type of encryption the far site uses. |
| Precedence Level       | (Video Endpoint Only) Applicable only on AS-SIP calls. AS-SIP servers support a "precedence level" that defines a call’s priority in terms of the order in which it is given access to network resources. |

### Device Alerts (Video Endpoint Only)

<p>| Errors                  | Endpoint error message, for example, GK Registration error. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warnings</td>
<td>Endpoint warning message, for example, Low Battery.</td>
</tr>
</tbody>
</table>

### Provisioning Details (Video Endpoint Only)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Provisioning Type</td>
<td>The last provisioning type that was used for this endpoint.</td>
</tr>
<tr>
<td>Last Provisioning Rule</td>
<td>The name of the last provisioning rule that was applied to this endpoint.</td>
</tr>
<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>
<tr>
<td>Last Bundled Profile Applied</td>
<td>The name of the last bundled profile that was applied to this endpoint.</td>
</tr>
</tbody>
</table>

**Provisioning Status**

- **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**.

**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.

**Last Attempt Date/Time**

The date and time, in the default format of `yyyy-mm-dd hh:mm:ss`, of the last provisioning message exchanged with the device.

**Failure Reason**

A text description of the reason the provisioning failed. Causes for failure include:

- The provisioning profile does not exist
- The provisioning profile does not include provisioning information
- The RealPresence Resource Manager system no longer manages the device
- A password for the device is set in the video endpoint system, and you must enter it in the RealPresence Resource Manager system
- The device is busy
- A network error occurred
- An incomplete transfer of provisioning information occurred
- Provisioning has timed out
- An internal error occurred on the device, and you must reboot it
- An unknown error occurred. Reboot the device.

**Log Message**

A read-only text box that contains messages related to the device provisioning status.
## Managing Endpoints and Peripherals

### Software Update Details (Video Endpoint Only)

<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>
<tr>
<td>Scheduled</td>
<td>The date and time, in the default format of <em>yyyy-mm-dd  hh:mm</em>, when the device software is scheduled to be updated.</td>
</tr>
<tr>
<td></td>
<td>This field is blank if the device is not scheduled for provisioning.</td>
</tr>
<tr>
<td>Last Attempt Date/Time</td>
<td>The date and time, in the default format of <em>yyyy-mm-dd  hh:mm:ss</em>, of the last software update message exchanged with the device.</td>
</tr>
<tr>
<td>Failure Reason</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 RealPresence 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>Log Message</td>
<td>A read-only text box that contains the log message text recorded during the execution of the software update.</td>
</tr>
<tr>
<td></td>
<td>Note that there are no log messages displayed for dynamically-managed endpoints.</td>
</tr>
</tbody>
</table>

### Endpoint Files (Phone Only)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Profiles</td>
<td>This file contains all the attributes applied to the selected phone.</td>
</tr>
<tr>
<td>Phone Files</td>
<td>This file contains the configuration data that set from the selected phone.</td>
</tr>
<tr>
<td>Web Files</td>
<td>This file contains the configuration data that set from the selected phone’s web GUI.</td>
</tr>
<tr>
<td>APP Logs</td>
<td>This file contains the APP information received by the selected phone.</td>
</tr>
<tr>
<td>Boot Logs</td>
<td>This file contains the phone’s boot information.</td>
</tr>
<tr>
<td>Crash Dump</td>
<td>This file contains the logs for crash dump.</td>
</tr>
<tr>
<td>Others</td>
<td>Other files such as a file containing phone’s address book.</td>
</tr>
</tbody>
</table>
Update Endpoint Model Definition

You can update the endpoint model definition in the RealPresence Resource Manager system to make the system always recognize the latest endpoint models.

If you do a local update, you need to download the endpoint definition file (polycom-device-types.zip) from the Polycom Support Center.

Restarting the RealPresence Resource Manager system is required to apply the updates.

To update endpoint model definition:

1. Go to Admin > Maintenance > Update Endpoint Model Definition.
2. Do one of the following to update the endpoint model definition.
   ➢ Click the Update from Local File button to upload the polycom-device-types.zip file.
   ➢ Click the Update from Polycom Hosted Server button to get the latest endpoint model files from the specified Polycom server.

   Web proxy server is not supported for connecting Polycom Hosted Server. You need to configure the access from the RealPresence Resource Manager system.

3. Restart the system.

Download Endpoint Files

You can download the endpoint files to your local machine. LOG files are cumulative, and content is appended with time stamps. The system creates a ZIP file if the log file is over 1024 KB by default. See Configure Your Phone Management Settings on how to set the size.

XML and CFG files are not cumulative. New files will replace old files.

You can download the endpoint files only from the RealPresence Resource Manager GUI. Polycom does not support downloading files in other ways.

You can view the endpoint files by opening them. RealPresence Resource Manager only can display text files correctly. Other files such as binary files can be opened, but can’t be displayed correctly.
To download endpoint files:

1. Go to Endpoint > Monitor View.
2. If needed, Click Filter to customize the endpoint list.
3. Select the phone and click View Details.
4. Go to the Endpoint Files panel.
5. Click Download to download the ZIP file to your local PC.

Add an Endpoint

You can manually add video endpoints or phones. The configurations are different.

Add a Video Endpoint or Find an Endpoint on the Network

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

This action is not supported for RealPresence Mobile, RealPresence Desktop, RealPresence Group systems, and RealPresence Immersive Studio systems.

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

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 Endpoint dialog, select a video endpoint as the Endpoint Type. For valid types, see Supported Endpoints and Peripherals. For endpoints not specified in the list, select Other.
3. Enter the IP Address of the endpoint.
4. Click Find Endpoint.
   - If the RealPresence Resource Manager system can find the endpoint on the network, the Add New Endpoint dialog 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, an error message of Endpoint Not Found appears.
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.

7. Complete the **Identification**, **Addresses**, and **Capabilities** sections of the **Add New Endpoint** dialog.

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 are ASCII only. Depending on the selected type, some of these fields may not be displayed or may not be editable.

8. (Optional) Click **Endpoint Group Association** and select the endpoint group to associate with. See **Working with Endpoint Groups** for details about endpoint groups.

9. Click **OK**.

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**.

For third-party endpoints, the HTTP URL, serial number, and DNS name are not captured during endpoint registration.

Once you’ve added an endpoint, you can associate it with a user. See **Edit a User**.

**Related Topics**

Supported Endpoints and Peripherals
Working with Endpoint Groups
Edit a User
Adding Endpoint Parameters

Adding Endpoint Parameters

The table explains the parameters for adding an endpoint.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification</strong></td>
<td></td>
</tr>
<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>GAB Display Name</td>
<td>Enter a name for the endpoint as it will appear in the Global Address Book.</td>
</tr>
</tbody>
</table>
| Site                | The network site for the endpoint. The system determines the site based upon IP address.  
                      | **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. |
| Serial Number       | The serial number (ASCII only) of the endpoint. The endpoint provides the serial number if it registered successfully or is managed. |
| Software Version    | The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed. |
| HTTP URL            | The management URL for the endpoint, if available (ASCII only). This URL enables 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.  
                      | For Cisco endpoints, you must manually enter the URL if you want to use the Manage function. |
| HTTP Port           | The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed. |
| 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.  
                      | If the user manages only one area, the endpoint will automatically be assigned to that area. |
| **Addresses**       |                                                                             |
| DNS Name            | The name for the endpoint as entered on the domain name server.              |
| SIP URI             | The address used to call the endpoint via SIP.  
                      | <username>@host(domain or IP):Port                                            |
### Managing Endpoints and Peripherals

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</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, email, 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. |
| **Capabilities**       | The communication protocols that the endpoint can support. Possible values include:  
  - **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based H.323 networks.  
  - **IP (SIP)** - A standard that defines the protocols used for multimedia communications on SIP networks.  
  - **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.  
  For endpoints with the type **Unknown**, select **H.323**.  
  The endpoint automatically provides the protocols if it registered successfully or is managed. |
| **Required MCU Service** | The MCU service selected for the endpoint to use. |
| **Capabilities Enabled** | Capabilities enabled on this endpoint. Options are:  
  - **MCU** - The endpoint can act as a control unit for multipoint conferences  
  - **Gateway** - The endpoint can act as a gateway for call management  
  The MCU provides the capability if it registered successfully or is managed. |
| **Monitoring Level**    | The monitoring level for the endpoint. Possible values include:  
  - **Standard.** This endpoint is monitored.  
  - **VIP.** This endpoint is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences. |
| **Available to Schedule** | Identifies if the endpoint is available when users are scheduling conferences. |
**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. In the **Endpoint Name** column, click the endpoint name that you want to edit.
   - As required, edit the **Identification**, **Addresses**, **Capabilities**, **Endpoint Group Association**, and **Configuration Profile Association** (phone only) sections of the **Edit Endpoint** dialog. For more information, see **View Endpoint Details**.
   - Note that many fields in this dialog are ASCII only.
3. Click **Update**.
   - The name of a dynamically-managed endpoint will be updated to the endpoint after the provisioning interval. To update other information, you need to use provisioning or change the information at the endpoint interface.

**Related Topics**

- [View Endpoint Details](#)

**Delete an Endpoint**

When you delete an endpoint, you remove the endpoint from the RealPresence Resource Manager system. You also delete all the associations with the endpoint.

**To delete an endpoint:**

1. Go to **Endpoint > Monitor View**
2. Select an endpoint you want to delete.
3. Click **Delete**.
4. If the endpoint is dynamically-managed, choose one of the following options:
   - **Delete Endpoint Only**: Deletes the endpoint
   - **Delete with dial string reservation**: Deletes the endpoint and any dial string reservations associated with the endpoint.
   - **Cancel**: Cancels the action.
5. Click **Delete** for other endpoints types.

**Change an Endpoint Group Association**

When you edit an endpoint, you can associate it with an endpoint group, delete its association with an endpoint group, or prioritize the associated endpoint groups in case of multiple ones.
To change the association from an endpoint to an endpoint group:

1. Go to Endpoint > Monitor View.
2. Click the endpoint name that you want to edit from the Endpoint Name column.
3. In the Edit Device dialog box, click the Endpoint Group Association tab.
   - To associate the endpoint to an endpoint group, select the name of the endpoint group from the drop-down list and click Add.
   - To delete the association, click Delete at the right end of each line of the endpoint group list.
   - To prioritize an association, click the Arrow buttons to deprioritize or prioritize it, or give it the lowest or highest priority.
4. Click OK.

Manage an Endpoint Owner

The endpoint owner is the user associated with the endpoint. You can manage an endpoint owner that uses scheduled management, but you cannot manage the owner of an endpoint that is dynamically-managed.

To manage an endpoint owner:

1. Go to Endpoint > Monitor View.
2. Select the endpoint of interest and click More > Manage Owner.
   - The Edit User dialog appears.
3. Edit any user properties you need.
4. Click OK.

Manage an Endpoint

You can navigate to the management interface of an endpoint from the RealPresence Resource Manager system. The RealPresence Resource Manager system only supports manage endpoint via HTTPS. HTTP is not supported. You need to enable HTTPS from the endpoint that you want to manage. For example, if you want to manage Polycom HDX or Polycom RealPresence Group Series, you need to enable HTTPS from Polycom HDX or Polycom RealPresence Group Series.

This function is not available for all endpoint types, including RealPresence Desktop, RealPresence Mobile, and CMA Desktop.

To manage an endpoint from the RealPresence Resource Manager system:

1. Go to Endpoint > Monitor View
2. Select the endpoint of interest.
3. Click .
   - A new browser instance opens and navigates to the web interface of the endpoint.
View Call Information

You can view an endpoint’s call information. You cannot view phone’s call information.

To view call information:
1. Go to Endpoint > Monitor View
2. Select the endpoint of interest.
3. Click More > Call Info to view the call information.

Call Information

This table explains the call information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Info &gt; Site</td>
<td></td>
</tr>
<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>
<tr>
<td>Sync</td>
<td></td>
</tr>
<tr>
<td>Call Type</td>
<td>Type of call, such as, H.323, SIP, ISDN, or POTS.</td>
</tr>
<tr>
<td>Call Info &gt; Call Details</td>
<td></td>
</tr>
<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>
</tbody>
</table>
### Field Description

- **Video Rate**: The video bandwidth negotiated with the far site.
- **Video Rate Used**: The actual video bandwidth used in the call to the far site.
- **Video Frame Rate**: Specifies the frame rate the endpoint is using.
- **Audio Protocol**: The audio connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include:
  - G.711
  - G.722
  - G.728
- **Audio Rate**: The audio bandwidth negotiated with the far site.

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

- **Total Packet Loss**: 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.
- **% Packet Loss**: 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.
- **Audio Packet Loss**: Specifies the audio packet loss for the currently active call.
- **Video Packet Loss**: Specifies the video packet loss for the currently active call.
- **Audio Jitter**: Specifies the audio jitter for the currently active call.
- **Video Jitter**: Specifies the video jitter for the currently active call.

### Call Info > Video Feed

- **Near Site**: The video feed from the endpoint.
- **Far Site**: The video feed from the endpoint to which the endpoint is connected.
- **Description**: A free-form text field (extended ASCII only) in which information about the endpoint can be added.
- **GAB Display Name**: Enter a name for the endpoint as it will appear in the Global Address Book.
- **Site**: The network site for the endpoint. The system determines the site based upon IP address.

**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.

- **Serial Number**: The serial number (ASCII only) of the endpoint. The endpoint provides the serial number if it registered successfully or is managed.
- **Software Version**: The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP URL</td>
<td>The management URL for the endpoint, if available (ASCII only). This URL enables 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. For Cisco endpoints, you must manually enter the URL if you want to use the Manage function.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.</td>
</tr>
<tr>
<td>Area</td>
<td>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. If the user manages only one area, the endpoint will automatically be assigned to that area.</td>
</tr>
<tr>
<td>Addresses</td>
<td></td>
</tr>
<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. &lt;username&gt;@host(domain or IP):Port</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, email, 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. |
### Managing Endpoints and Peripherals

#### View an Endpoint’s Video Feed

You can only view the video feed from the following endpoints:

- Polycom HDX system
- Polycom RealPresence Group Series system
- TANDBERG
- VSX-Series

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

1. Go to **Endpoint > Monitor View**.
2. Select the endpoint of interest.
3. Click **More > Call Info**.
4. Click the **Video Feed** tab to see the video feed from the near and far site.
Clear an Endpoint Help Request

This action is only applicable for an HDX system.

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 More > Clear Help.
   The Confirm Endpoint Help Clear dialog 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 and click Send.
   The Endpoint list is updated and alerts for the endpoint are cleared.

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.

This action is not applicable for RealPresence Mobile, RealPresence Desktop, CMA Desktop systems, or phones.

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

1. Go to Endpoint > Monitor View
2. Select the endpoint of interest.
   If the endpoint can receive text messages, a Send Message option appears in the More menu.
3. Click More > Send Message.
4. In the Send Message to Endpoint dialog, enter a text message and click OK.
   The message is sent to the endpoint.

Reboot an Endpoint

An endpoint must be online inside the firewall to get rebooted from the RealPresence Resource Manager system.
To reboot an endpoint from the RealPresence Resource Manager system:

1. Go to Endpoint > Monitor View
2. Click Switch Selection Types to enable multiple select.
3. Select the one or more endpoint(s) of interest.
4. Click More > Reboot Device.
5. To confirm the request, click OK.

**Associate a User with an Endpoint**

This action is available for endpoints that are not dynamically managed such as RealPresence DMA system-synchronized endpoints and phones. For example, if you associate a user with a RealPresence DMA system-synchronized endpoint, you can manage that endpoint. Endpoints that are associated with user (or room) can be scheduled into conferences.

To associate an endpoint to a user:

1. Go to Endpoint > Monitor View
2. Select the endpoint of interest.
3. Click More > Associate User.
4. In the Last Name or Room Name field or the First Name field, enter all or part of the user’s last name or first name and click Search.
   - The system displays the list of user or rooms that meet your search criteria.
5. Select the user of interest.

**Search for Endpoints in a Range of IP Addresses**

You can search for endpoints within a range of IP addresses. This search will only include endpoints that are not dynamically managed, which are not displayed in the current endpoints list. The purpose of this function is to provide a quick approach to find out those non-dynamically managed endpoints, so that RealPresence Resource Manager can add the endpoints in a batch.

Phones do not support this feature.

To search for a set of endpoints within a range of IP addresses:

1. Go to Endpoint > Monitor View and click More > Search Endpoints.
2. In the Search Endpoints dialog, 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.
Working with Endpoint Groups

Endpoint groups are logical collections of endpoints and are mainly used for phones' provisioning. Users with the Endpoint Admin or System Setup permission can manage endpoint groups.

Add an Endpoint Group

You can define a new endpoint group by selecting a list of existing endpoints in the RealPresence Resource Manager system.

To add an endpoint group:

1. Go to Endpoint > Endpoint Groups.
2. Click Add.
3. Enter a name and description for this endpoint group.
4. In the Endpoint Association tab, select the endpoints you want to include in the group from the Available table and click the down arrow to move them to the Selected table.
5. In the Phone Configuration Profile Association tab, select a profile from the Configuration Profile Association drop-down list.
6. Click the Save and Apply button to associate this profile to the endpoint group.
7. Repeat step 5 and step 6 to associate more profiles.
   The associated configuration profiles only apply to the phones in the endpoint group.
8. Do one of the followings to save the changes:
   - Click Save and Apply to apply the phone configuration profiles to the on-line phones in this endpoint group immediately. This operation may reboot the phones. This operation only applies this time changes to the phones. It does not apply previous changes to the phones.
   - Click Save to only save the change. The RealPresence Resource Manager system will not apply the changes until the next polling interval.

Edit an Endpoint Group

You can edit an endpoint group and change its associated endpoints and phone configuration profiles at anytime.

To edit an endpoint group:

1. Go to Endpoint > Endpoint Groups.
2. Do one of the followings to open the Edit Endpoint Group dialog:
   - Click the endpoint group hyperlink.
   - Select the endpoint group and click Edit.
3. Make changes as needed.
4. Do one of the followings to save the changes:
Managing Endpoints and Peripherals

- Click **Save and Apply** to apply the phone configuration profiles to the on-line phones in this endpoint group immediately. This operation may reboot the phones. This operation only applies this time changes to the phones. It does not apply previous changes to the phones.
- Click **Save** to only save the change. The RealPresence Resource Manager system will not apply the changes until the next polling interval.

**Copy an Endpoint Group**

You can create a new endpoint group by cloning an existing endpoint group and making necessary changes.

**To create an endpoint group based on a cloned endpoint group:**

1. Go to **Endpoint > Endpoint Groups**.
2. Select an endpoint group and click **Clone**.
3. In the **Copy Endpoint Group** dialog, enter a name and description for the new endpoint group.
4. Edit the associations as needed.
5. Do one of the followings to save the changes:
   - Click **Save and Apply** to apply the phone configuration profiles to the on-line phones in this endpoint group immediately. This operation may reboot the phones. This operation only applies this time changes to the phones. It does not apply previous changes to the phones.
   - Click **Save** to only save the change. The RealPresence Resource Manager system will not apply the changes until the next polling interval.

**Customize the Endpoint Group List**

You can customize your endpoint group list by using filter.

**To customize the Endpoint Group list:**

1. Go to **Endpoint > Endpoint Groups**.
2. Click **Filter** to filter endpoint groups by **Endpoint Group Name** or **Modified By** condition.
3. Press **Enter** to do the search.
4. Click **Reset** if you want to do another search.
5. Enter a key word in the **Search** field beside **Filter** to search the key word among the filter results.

**Reboot Phones in an Endpoint Group**

You can reboot all the phones belonging to an endpoint group.

**To reboot phones:**

1. Go to **Endpoint > Endpoint Groups**.
2. Select an endpoint group.
3 Select **More > Reboot Phones**.
4 Click **OK** to confirm the reboot.

**Set an Active Directory Password for Phones in an Endpoint Group**

You can only set an active directory password for Polycom phones that support REST API, such as RealPresence Trio and Polycom VVX phones.

**To set active directory password for phones in an endpoint group:**

1. Go to **Endpoint > Endpoint Groups**.
2. Select an endpoint group.
3. Click **More > Change Phone AD Password**.
4. Enter a new password.
5. Click **OK**.

After the operation is completed, click the **Download Detailed Report** button to view the detailed logs.

**Refresh an Endpoint Group**

Refresh the **Endpoint Group** page to see the endpoint group changes make by other users.

**To refresh the endpoint group page:**

1. Go to **Endpoint > Endpoint Groups**.
2. Click **Refresh**.

**View Endpoint Group Details**

The detail information containing name, description, and its associations are display on the right.

**To view details of a profile:**

1. Go to **Endpoint > Endpoint Groups**.
2. Select an endpoint group and click **View Details**.

**Delete an Endpoint Group**

If you delete an endpoint group with endpoints that are associated with phone configuration profiles, all the associations will be removed.

**To delete an endpoint group:**

1. Go to **Endpoint > Endpoint Groups**.
2 Select an endpoint group and click **Delete**.

3 Click one of the followings to confirm the deletion:
   - **Delete and Apply**: Apply the phone configuration profile associations deletion to the related Intranet online phones now. This may reboot the phones.
   - **Delete**: Delete the endpoint group and all its endpoint and profile associations. The deletion applies to the related phones automatically at the next polling interval.

**Set an Endpoint Group to Top Priority**

This operation sets the selected endpoint group to the highest priority group in its all associated phones. For each associated phone, the configuration profiles belonging to the selected endpoint group will have the highest priority comparing to other endpoint group associated configuration profiles for this phone.

**To set an endpoint group to top priority:**

1 Go to **Endpoint > Endpoint Groups**.
2 Select an endpoint group.
3 Select **More > Set Top Priority**.
4 Click **OK**.
   The endpoint group becomes the group with the highest priority in all its associated endpoints.

**Set Default Endpoint Group**

This operation sets the default endpoint group(s) for new auto-added phones. When a new phone is added to the system automatically via HTTP/HTTPS, the system adds the new phone to the specified default endpoint group(s). The system apply the configuration profiles associated with the default endpoint group(s) will be applied to the auto-added phones once phones are added to the RealPresence Resource Manager system.

**To set default endpoint group(s):**

1 Go to **Endpoint > Endpoint Groups**.
2 Select **More > Set Default Endpoint Group**.
3 Select an endpoint groups from the **Endpoint Groups** drop-down list.
4 Click **Add**.
5 Repeat step 3 and step 4 to add more endpoint groups.
6 (optional) Click **Arrow** to adjust the priority of the specified endpoint groups for the phones that will be auto-added.
7 Click **OK**.
Monitoring and Managing Peripherals

If an endpoint is provisioned by the RealPresence Resource Manager system and this endpoint has one or more peripherals connected, the peripherals can be added and provisioned and you can view information about the peripherals.

Monitor Peripherals

Use the Peripherals View to monitor peripherals connected to dynamically managed endpoints.

» Go to Endpoint > Peripherals View to view peripherals.

Customize the Peripheral List

You can customize the peripherals that you want to display by using filter.

To Customize the Peripheral List:

1  Go to Endpoint > Peripherals View.
2  Click Filter .
3  Use the filter choices to display other views of the Endpoint list, which include:
    ➢ Endpoint Type  Filters the list by type.
    ➢ Paired Endpoint  Filters the list by the endpoint to which the peripherals are connected.
    ➢ IP Address    Filters the list by IP address entered.
    ➢ Hardware Version  Filters the list by hardware version entered.
    ➢ Software Version  Filters the list by software version entered.
4  Press Enter to do the search.
5  Click Reset if you want to do another search.

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.
Managing Endpoints and Peripherals

Link to the Management Web Interface of a Peripheral

You can navigate to the management interface of a peripheral from the RealPresence Resource Manager.

Link to the Management Web Interface of a Peripheral:

1. Go to Endpoint > Peripherals View
2. Select the peripheral of interest.
3. Click More > Manage.

A new browser instance opens and navigates to the web interface of the endpoint.

Deleting a Peripheral

When an endpoint is deleted, the peripherals connected with this endpoint are removed automatically. When a peripheral is no longer connected to an endpoint, this peripheral is not in the Peripherals View list. You cannot delete peripherals manually.

Display Applications

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

To display applications:

1. Go to Endpoint > Peripherals View and select a peripheral.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The state of the peripheral. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Connected - Peripheral is connected to the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Disconnected - Peripheral is turned off or no longer connected to the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Error - Endpoint reports an error with the peripheral.</td>
</tr>
<tr>
<td></td>
<td>• Blank - Endpoint is not reporting that the peripheral is connected.</td>
</tr>
<tr>
<td>Paired Endpoint</td>
<td>Name of the endpoint to which the peripheral is connected or Not Paired. The Not Paired 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>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>
2. Click More > Display Applications. The Applications Installed on dialog for the selected peripheral appears.
   - Application Name: Name of the peripheral application.
   - Version: Version of the peripheral application.

3. Click OK.

**Peripheral Software Update**

The following peripherals can be updated separately via the RealPresence Resource Manager system:
- HDX Touch Control
- RealPresence Group Series Touch Control
- RealPresence Touch

Other peripherals can be updated with their connected endpoints.

**To update a peripheral:**

1. Go to Endpoint > Dynamic Management > Upload Software Updates.
2. Select one of the Touch Control peripherals from the Endpoint Type drop down list.
3. Click Add to upload the software update file.

**Download an Endpoint Inventory Report**

You can download an inventory report of endpoints if you have the Admin role.

**To download an endpoint inventory report:**

1. Navigate to Endpoint > Monitor View.
2. Click Download. The file is saved to the default download folder of your browser.

**Endpoint Inventory Report**

This report is in *.CSV format and includes the following information about each endpoint:

<table>
<thead>
<tr>
<th>Endpoint Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>The type of device.</td>
</tr>
<tr>
<td>Model</td>
<td>The model number of the device</td>
</tr>
</tbody>
</table>
| Manage Mode        | Describes if the device is dynamically managed:
|                    | • NON_DYNAMIC means it is not dynamically managed. |
|                    | • DYNAMIC means the endpoint is dynamically managed. |
### Managing Endpoints and Peripherals

<table>
<thead>
<tr>
<th>Endpoint Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner Name</td>
<td>The user associated with the device.</td>
</tr>
<tr>
<td>Endpoint Group</td>
<td>The endpoint group that the endpoint belongs to.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Endpoint's MAC address.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The assigned IP address of the device.</td>
</tr>
</tbody>
</table>
| ISDN Video Number       | 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 RealPresence Resource Manager system only supports native ISDN. |
| E.164 Number            | The value for the E.164 number associated with this device.         |
| H323 Alias              | 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 then the H323 ID. |
| SIP URI                 | The SIP URI address for the device.                                  |
| Software Version        | The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed. |
| Serial Number           | The serial number (ASCII only) of the device. The device provides the serial number if it registered successfully or is managed. |
| Sites                   | The network site for the device. By default, devices are added to the Primary Site.  
**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. |
| GK IP                   | The IP address of the gatekeeper to which the device is registered. |
| SIP server IP           | The IP address of the SIP server to which the device is registered. |
Supported Endpoints and Peripherals

The RealPresence Resource Manager system supports managing and monitoring both Polycom and third-party endpoints.

Supported Polycom Endpoints

The table describes the RealPresence Resource Manager system support for Polycom endpoints based on endpoint type and category of support.

The Polycom Telepresence M100 systems register as endpoint type of Other. As such, the RealPresence Resource Manager can schedule and perform limited monitoring of these systems.

<table>
<thead>
<tr>
<th>Polycom Endpoint Types</th>
<th>Global Address Book Access</th>
<th>Dynamic Management</th>
<th>Scheduled 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 Desktop</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>Y</td>
</tr>
<tr>
<td>RealPresence Mobile</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>Y</td>
</tr>
<tr>
<td>CMA Desktop</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>Y</td>
</tr>
<tr>
<td>Polycom CX5100</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>RealPresence Group Series (must be dynamically managed)</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>RealPresence Immersive Studio system (must be dynamically managed)</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>
## Supported Endpoints and Peripherals

<table>
<thead>
<tr>
<th>Polycom Endpoint Types</th>
<th>Global Address Book Access</th>
<th>Dynamic Management</th>
<th>Scheduled 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 Debut</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>RealPresence Centro</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>Polycom Pano</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>HDX Series (dynamic management mode)</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>
<td>N</td>
</tr>
<tr>
<td>HDX Series (scheduled management mode)</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>VVX 1500 Series (dynamic management mode)</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>VSX Series</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>N</td>
</tr>
<tr>
<td>QDX Series</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>N</td>
</tr>
</tbody>
</table>

a. Polycom RealPresence Group Series systems must be dynamically managed. If a RealPresence Group Series system is not dynamically managed, it can still connect to the Global Address Book.
b. The Polycom VVX 1500 cannot be dynamically provisioned when it is behind a Polycom VBP-ST firewall.
c. Dynamic Management and Scheduled Management are mutually exclusive functionality.
d. 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 asked to perform dialing. Some endpoints, such as CMA Desktop clients and VVX systems require external MCU resources for dial-in conferences.
e. Standard RealPresence Resource Manager monitoring does not involve using SNMP. It includes endpoint monitoring (online/offline status) and alerts.
f. 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.
g. 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.
Supported Polycom Peripherals

The following peripherals are supported. The system can only monitor them.

- Polycom Touch Control
- Polycom RealPresence Touch Control
- Polycom EagleEye Producer
- Polycom EagleEye Director
- Polycom EagleEye Director II

People count information available from a Polycom EagleEye Producer or EagleEye Director II camera is available in the Call Detail Report.

Supported Third-Party Endpoints

The table describes the RealPresence Resource Manager system support for third-party endpoints based on endpoint type and category of support.

<table>
<thead>
<tr>
<th>Endpoint Type</th>
<th>Global Address Book Access</th>
<th>Dynamic Management</th>
<th>Scheduled 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>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco T150 MXP</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>N</td>
</tr>
<tr>
<td>Cisco 95 MXP</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>
</tr>
<tr>
<td>Cisco C Series</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>
</tr>
<tr>
<td>Cisco MX Series</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>
</tr>
<tr>
<td>Cisco EX Series</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>
</tr>
<tr>
<td>Cisco SX Series</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>
</tr>
<tr>
<td>LifeSize Team and Express</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>
</tr>
</tbody>
</table>

h. Supported behind a Polycom VBP, Polycom RealPresence Access Director or Acme SBC device with Access Proxy enabled.
Managing Third-Party Endpoints

The RealPresence Resource Manager system includes additional command and control for select TANDBERG C Series, Cisco SX series, Cisco EX series, and LifeSize Team and Express endpoints. The RealPresence Resource Manager system can:

- Send a Reboot command to these endpoints.
- Discover these endpoints 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.
**Scheduled Provisioning of Third-party Endpoints**

You can set up scheduled provisioning profiles for third-party endpoints. See Scheduled Endpoint Provisioning for information on implementing scheduled provisioning of endpoints.

See the endpoint documentation for more information about endpoint configuration fields, acceptable values, restrictions in changing passwords for a specific endpoint.

**Managing Cisco Endpoints**

The RealPresence Resource Manager can provision Cisco endpoints using HTTP or HTTPS. Cisco endpoints can access the Polycom Global Address Book via the RealPresence Resource Manager system.
Enable Cisco Endpoints Global Address Book Access

With the RealPresence Resource Manager system, users of the Cisco endpoints can access the Polycom Global Address Book, so they can see the endpoints in the Global Address Book.

Even if the Global Address Book is password protected, Cisco endpoints are not required to provide a password. They have unrestricted access to the Global Address Book.

When your Cisco endpoints are registered to a Cisco address book, the endpoint’s directory status will display as unregistered on the RealPresence Resource Manager system Endpoint > Monitor View page.

To access the Polycom Global Address Book access:

1. On Cisco endpoints, go to System Configuration> Phone Book Server.
2. Enter the information required for directory set up including the Polycom Global Address Book/RealPresence Resource Manager system IP address and the path.
   For example, http://<RPRM_IP_ADDRESS>/TMS/Public/external/phonebook/PhoneBookService.asmx
3. Wait for the connections to take effect.
4. 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 Cisco Endpoints

You can set up scheduled provisioning profiles for third-party endpoints. See the appropriate product documentation for more information about these endpoint configuration fields and their acceptable values. See Scheduled Endpoint Provisioning for information on implementing scheduled provisioning of endpoints.

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

Enable HTTPS for Cisco Endpoints Management

RealPresence Resource Manager system supports using HTTPS when managing a Cisco endpoint.

The following Cisco endpoints are supported with HTTPS (and HTTP):

- Cisco C series
- Cisco SX series
- EX series
- Cisco MXP series

The Cisco T-150 series does not support HTTPS.

By default, the RealPresence Resource Manager system will try both HTTP and HTTPS when accessing a Cisco endpoint. For better performance, you can enable the system to try your preferred protocol first.

When HTTPS is used, the Cisco endpoint cannot accept a software update.
To configure the system to use HTTPS when managing Cisco endpoints:

1. Navigate to **Endpoint > Scheduled Management > Endpoint Management Settings**.
2. Under **Cisco Endpoint Management**, select the **Use HTTPS** check box.

**Managing LifeSize Endpoints**

The RealPresence Resource Manager system can provision the LifeSize endpoints and their passwords.

**Enable LifeSize Endpoints Management**

To facilitate LifeSize endpoints management, you must enable the **Default Passwords for LifeSize Endpoint Management** option and enter the SSH and web UI passwords for the LifeSize endpoints.

Please see the LifeSize documentation for password parameters.

To enable LifeSize endpoint management:

1. On the RealPresence Resource Manager system, go to **Endpoint > Scheduled Management > Endpoint Management Settings**.
2. In the **Default Passwords for LifeSize Endpoint Management** section of the **Endpoint Management Settings** page, enable **Use Default Passwords**.
3. Enter the **Password for 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 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 password.

**Scheduled Provisioning of LifeSize Endpoints**

The RealPresence Resource Manager system can provision many fields for LifeSize Team and Express endpoints. See the appropriate product documentation for more information about these endpoint configuration fields and their acceptable values.
See the Scheduled Endpoint Provisioning for information on implementing scheduled provisioning of endpoints.
Managing Polycom Software Endpoints

You can distribute Polycom RealPresence Desktop for use in specific environments.

**Distributing Polycom RealPresence Desktop for Windows Systems**

Polycom provides you multiple options to deploy the RealPresence Desktop client to users. You must implement DNS lookup and Windows authentication for single sign-on. On a Windows systems, you must sign in with administrative privileges to install the Polycom RealPresence Desktop.

**Distribute the Client via an E-mail Link**

You can an e-mail with the link for the client to users.

To distribute the client via an e-mail link:

1. Copy and paste the link from the Downloads page into an e-mail to be sent to users.
2. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the e-mail to users.

**Distribute the Client via the Management System**

You can provide users access to the RealPresence Resource Manager system, from which they can download the client.

To distribute the client via the management system:

1. Copy and paste the link from the Downloads page into an e-mail to be sent to users.
2. Include usernames and passwords (as required) in the e-mail to users and instruct them to access the Downloads link.

**Distribute the 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 distribute the client via a desktop management or group policy object:

1. 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.

2. Include the command for executing the file in an e-mail to be sent to users. For example:
   
   ```
   C:\temp\RPD.exe"/s /v"/qn SBSERVERTYPE=2 SBSERVERADDRESS=nnn.nnn.nnn.nnn
   ```

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

Distribute the Client via a ZIP File

You can distribute the .exe installation file and send it in an e-mail to users.

To distribute the client via ZIP file:

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

2. 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.

3. Zip the .exe installation file and send it in an e-mail to users.

Have users download the client from the Polycom support page

You can tell users to download a Polycom RealPresence Desktop from Polycom support.

With this option, you also need to e-mail users the IP address of the RealPresence Resource Manager and the required username and password.

Distributing Polycom RealPresence Desktop for MAC Systems

Polycom provides you multiple options to deploy the RealPresence Desktop client to users.

On a MAC system, the user installing the client must sign in with administrative privileges. You need to have implemented DNS lookup and MAC authentication for single sign-on.

Download the Client from the Polycom Support Page

You can download the installation package from the Polycom support center. With this option, you also need to e-mail users

To download the client from the Polycom Support Center:


2. Select a Polycom RealPresence Desktop to download.

3. Send e-mails to users with the RealPresence Resource Manager IP address, username, and password.
Distribute the Client for MAC client via an E-mail Link

You can copy the link for the client for MAC clients from the RealPresence Resource Manager system Downloads page into an e-mail that you can send to users.

To distribute the client for MAC client via an e-mail link:

1. Copy and paste the client for MAC link (e.g., http://10.47.9.136/SoftUpdate/vvl/CMADesktopMac_5_2_3/CMADesktop.dmg) from the Downloads page into an e-mail to be sent to users.
2. Include the RealPresence Resource Manager system IP address, usernames, and passwords (as required) in the e-mail to users.

Distribute the 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 distribute the MAC client via the management system,

1. Copy and paste the IP address of the client system into an e-mail to be sent to users.
2. Include usernames and passwords (as required) in the e-mail to users and instruct them to access the Downloads link.

Distribute the Mac Client via a .dmg File

You can distribute the installation package via a .dmg file.

To distribute the installation package via a .dmg file:

1. Include the RealPresence Resource Manager system IP address, usernames, and passwords (as required) in the e-mail to users.
2. 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.
3. Send the .dmg file in an e-mail to users.
Scheduled Endpoint Management

Scheduled management enables you to push software updates and provisioning profiles to endpoints at intervals that you define. You can use scheduled management features to manage Polycom as well as third-party endpoints.

Scheduled management uses server-to-client communication over HTTP or HTTPS. This management technique is more appropriate for corporate networks where both the RealPresence Resource Manager and all endpoints are behind the same firewall.
Scheduled Endpoint Provisioning

You can schedule endpoint provisioning for an individual endpoint or group of endpoints. You can have provisioning scheduled to occur immediately or for a date and time in the future. The provisioning data is sent in XML format over a HTTP or HTTPS connection.

You can schedule provisioning for an unlimited number of endpoints, but the system may limit the number of active provisioning processes. Some provisioning operations may reboot the endpoint.

You must have Device Administrator or Area Administrator role to use scheduled provisioning features.

Supported Endpoints for Scheduled Management

In order to be provisioned, an endpoint’s system name cannot exceed 36 characters or the provisioning will fail.

Scheduled provisioning is available for these endpoint types:

- Polycom VSX Series endpoints
- Polycom HDX Series—Polycom HDX systems that are not dynamically managed (are not configured to use a provisioning server)
- Polycom QDX Series endpoints
- Selected Cisco endpoints—Cisco 95, Cisco 150 MXP, Cisco C series, Cisco EX series, and Cisco SX endpoints
- LifeSize

Scheduled Endpoint Management Settings

When you use scheduled management for endpoints, you can configure several options that make management easier.

Enable Automatic Registration Synchronization

You can configure the RealPresence Resource Manager system to send registration server address 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.
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. Pre-existing endpoints cannot be registered to GDS automatically. If automatic discovery and configuration is not successful, you can manually add endpoints.

The RealPresence Resource Manager system only supports Automatic Registration Synchronization for Polycom and selected third-party endpoints that are not dynamically managed.

To enable Automatic Registration Synchronization of endpoints:

1. Go to Endpoint > Scheduled Management > Endpoint Management Settings.
2. In the Automatic Registration Synchronization section, select Synchronize endpoint registration and click Update.

After you have changed this setting, all endpoints you added are automatically provisioned.

**Enable Use HTTPs for Cisco Endpoint Management**

When Use HTTPs is checked, the RealPresence Resource Manager system will check for an HTTPs connection first when managing Cisco endpoints. If it is not checked, the system checks for an HTTP connection first.

To set HTTPs as a preference for Cisco endpoints:

1. Navigate to Endpoints > Scheduled Management > Endpoint Management Settings.
2. In the Cisco Endpoint Management section, select the Use HTTPs check box.

When this check box is selected, the RealPresence Resource Manager system will check for an HTTPs connection first when managing Cisco endpoints.

**Use a Common Password for Endpoints**

This feature enables you to manage endpoints with scheduled management (provisioning and software updates) that have the same global administrative password.

If you set a common password for endpoints, access to password-protected data within endpoints is granted if the specified common password matches the endpoints’ Administrator Password. Setting a common password does not reset the administrative password on endpoints.

To set a common password for endpoints:

1. Go to Endpoint > Scheduled Management > Endpoint Management Settings.
2. In the Common Password section, select Use a Common Password.
3. Enter the common User Name and a common password in the Password and Verify Password fields and click Update.

**Disable Common Password for Endpoints**

You can disable common passwords for endpoints.
To disable common passwords for endpoints:

1. Go to Endpoint > Scheduled Management > Endpoint Management Settings.
2. In the Common Password section, clear Use a Common Password and click Update.

Creating 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 a endpoint for provisioning. Create a different profile for each endpoint type.

You must have the device administrator role to modify provisioning profiles. Users with the role of area administrator cannot modify provisioning profiles.

Some examples of when to use scheduled provisioning profiles:

- 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 purpose, 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.

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

Add a Scheduled Provisioning Profile

You must create a profile for the endpoint type you want to provision.

To add a scheduled provisioning profile:

1. Go to Endpoint > Scheduled Management > Provisioning Profiles.
2. In the Provisioning Profiles page, click Add.
3. In the Add Profile dialog, select the Endpoint Type for the provisioning profile, enter a name for the profile, and click OK.
4. On the Edit Scheduling Provisioning Profile dialog,
   - For Polycom endpoints and LifeSize, select Provision This Page.
     Each page has a Provision This Page check box. When this check box 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 selected, or the system returns an error stating.
   - For Cisco endpoints, select the parameters that you want to provision on each page. You can check the Select All check box to select all the parameters on each page.
5. Complete the settings on this page as needed.
6. Click OK.
Scheduled Endpoint Provisioning

**Edit a Scheduled Provisioning Profile**

You can edit an existing provisioning profile. You cannot rename an existing profile. If you want to change the name of a provisioning profile, you can clone a profile and rename it.

**To edit a scheduled provisioning profile:**
1. Go to **Endpoint > Scheduled Management > Provisioning Profiles**.
2. In the **Provisioning Profiles** list, select the profile of interest and click **Edit**.
3. As needed, update the parameters on each page.
4. Click **OK**.

**Clone a Scheduled Provisioning Profile**

If you want to rename an existing provisioning profile or create a new profile based on an existing profile, you can use the **Clone** action.

**To clone a scheduled provisioning profile:**
1. Go to **Endpoint > Scheduled Management > Provisioning Profiles**.
2. Select a profile and click **Clone**.
3. In the **Clone Profile** dialog, enter a name for the new profile and click **OK**.
   
   The provisioning profile appears first in the updated **Provisioning Profiles** list.
4. Edit the this profile as needed.
5. Click **OK** to save the changes.

**Delete a Scheduled Provisioning Profile**

You can delete a provisioning profile at any time. Deleted profiles will no longer be sent during scheduled provisioning updates.

**To delete a scheduled provisioning profile:**
1. Go to **Endpoint > Scheduled Management > Provisioning Profiles**.
2. In the **Provisioning Profiles** page, select a profile and click **Delete**.
3. Click **OK** to confirm the deletion.

**Scheduling Endpoints for Provisioning**

You can schedule provisioning for an unlimited number of endpoints, but the system may limit the number of active provisioning processes. Keep in mind that provisioning may reboot the endpoint.

You must have Device Administrator or Area Administrator role to use scheduled provisioning features.
Scheduled Endpoint Provisioning

- 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**.

**View a List of Eligible Endpoints**

You can view a list of endpoints registered to the RealPresence Resource Manager system that are eligible for scheduled provisioning.

You must have Device Administrator or Area Administrator role to use scheduled provisioning features. You must have already created a provisioning profile to use before you can schedule a provisioning update for an endpoint.

**To view a list of eligible endpoints:**

1. Go to **Endpoint > Scheduled Management > Provisioning**.
2. As needed, click **Filter** to filter the **Endpoint** list. The filter choice for endpoint types that can be scheduled for provisioning. Possible values include:
   - **HDX Series**—Displays the Polycom HDX systems operating in scheduled management mode.
   - **Cisco®**
   - **LifeSize®**
   - **QDX Series**
   - **V and VSX Series**

**Eligible Endpoints Information**

The **Endpoint** list in this view has the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the endpoint’s last provisioning process. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Pending</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Failed</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Clear</strong></td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>The system name of the endpoint.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of endpoint. Scheduled provisioning is only available for the endpoints types listed in this table as <strong>Filter</strong> selections.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the endpoint.</td>
</tr>
<tr>
<td>Last</td>
<td>The date and time of the endpoint’s last provisioning, unless its status has been cleared.</td>
</tr>
</tbody>
</table>
Scheduled Endpoint Provisioning

You can schedule provisioning profiles to be sent to endpoints at times you specify.
You must have Device Administrator or Area Administrator role to use scheduled provisioning features.

To schedule an endpoint for provisioning:

1. Go to Endpoint > Scheduled Management > Provisioning.
2. As needed, click Filter to filter the endpoint list.
3. Select the endpoints that you want to schedule provisioning updates.
4. Click More > Provision.
5. In the Scheduled Provisioning Profiles dialog, 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 Update

You can monitor the status of scheduled provisioning updates. 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 canceled.
Profile statuses include: Pending, Failed, Success, and Clear.
You must have Device Administrator or Area Administrator role to use scheduled provisioning features.

To check the status of a scheduled provisioning:

1. Go to Endpoint > Scheduled Management > Provisioning.
2. As needed, click Filter to filter the endpoint list.
3. Select the endpoint of interest.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>When the endpoint is scheduled for provisioning, this field shows the provisioning profile to be used for the scheduled provisioning process.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>When the endpoint is scheduled for provisioning, this field shows the date and time for the next scheduled provisioning process.</td>
</tr>
</tbody>
</table>
Scheduled Endpoint Provisioning

4. Click **View Details** to open the **Device Details** section.
5. Expand the **Provisioning Details** tab.
6. View the **Status** field to see the current status of the update.

**Clear the Status of Scheduled Provisioning**

You can reset the provisioning status so you can better monitor succeeding provisioning updates. For example, you can clear all profile Success statuses.

You must have Device Administrator or Area Administrator role to use scheduled provisioning features.

To clear the status of a scheduled provisioning:

1. Go to **Endpoint > Scheduled Management > Provisioning**.
2. As needed, click **Filter** to filter the endpoint list.
3. Select the endpoint of which you want to clear the status.
4. Click **More > 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**.

You must have Device Administrator or Area Administrator role to use scheduled provisioning features.

To cancel a pending scheduled provisioning:

1. Go to **Endpoint > Scheduled Management > Provisioning**.
2. As needed, click **Filter** to filter the endpoint list.
3. Select the endpoints of interest.
4. Click **More > Cancel Provision**.
   The provisioning operation is canceled and the provisioning status returns to **Clear**.

**Endpoint Fields for Scheduled Provisioning Profiles**

The following table shows the fields you can configure when adding a new scheduled provisioning profile for a Polycom endpoint. You may find more implementation details about these fields in the endpoint system documentation.

For information about third-party endpoint fields, consult the respective documentation.
### General Settings > System Settings > System Settings 1

<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>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</td>
<td>Y</td>
<td>Y</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</td>
<td>Y</td>
<td>N</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</td>
<td>Y</td>
<td>Y</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</td>
<td>Y</td>
<td>N</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</td>
<td>Y</td>
<td>Y</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</td>
<td>Y</td>
<td>Y</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</td>
<td>Y</td>
<td>Y</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</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

### General Settings > System Settings > System 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>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</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Display Time in Call</td>
<td>Displays time that the current call has been connected</td>
<td>Y</td>
<td>Y</td>
<td>Y</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</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Call Detail Report</td>
<td>Collects call data.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Recent Calls</td>
<td>Provides navigational tool for call history.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Color Scheme</td>
<td>Enables the customization of the look of the system with five different color schemes.</td>
<td>N</td>
<td>Y</td>
<td>N</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>N</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Scheduled Endpoint Provisioning

#### General Settings > Home Screen Settings > Home Screen Settings 1

Home screen settings cannot be provisioned for Polycom QDX endpoints.

<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>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>N</td>
</tr>
</tbody>
</table>

#### General Settings > Home Screen Settings > Home Screen 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>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>N</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>
</tbody>
</table>
### Scheduled Endpoint Provisioning

#### Field

<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>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.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>The meeting password must not contain spaces.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You cannot provision this setting for Polycom VSX systems.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Web Access</td>
<td>Specifies that the endpoint system can be accessed via it’s web interface.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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></td>
</tr>
<tr>
<td>Enable Telnet Access</td>
<td>Specifies that the endpoint system can be accessed via a telnet session.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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></td>
</tr>
<tr>
<td>AES Encryption</td>
<td>Specifies how to encrypt calls with other sites that support AES encryption.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>• Off—AES Encryption is disabled.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When Available—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don’t support it.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable SNMP Access</td>
<td>Specifies that the endpoint system can be accessed via an SNMP monitoring system.</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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></td>
</tr>
</tbody>
</table>
### General Settings > Date and Time 1

<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>Date Format</td>
<td>Specifies the preferred format preference for the date and time display and lets you enter your local date and time.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Format</td>
<td></td>
<td>Y Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Month</td>
<td></td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Day</td>
<td></td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td></td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hour</td>
<td></td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minute</td>
<td></td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AM/PM</td>
<td></td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Adjust for Daylight Saving Time</td>
<td>Specifies the daylight savings time setting. When this setting is enabled, the system clock automatically changes for daylight saving time.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Difference from GMT</td>
<td>Specifies the time difference between GMT (Greenwich Mean Time) and the endpoint system’s location.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Server</td>
<td>Specifies connection to a time server for automatic system time settings.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<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 Y Y</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Video Network > IP Network > Call 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>Enable IP H.323</td>
<td>Enables the system to make IP calls</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable H.239</td>
<td>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.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Transcoding</td>
<td>Specifies whether the system enables 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.</td>
<td>Y Y N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISDN Gateway</td>
<td>Enables users to place IP-to-ISDN calls through a gateway.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Gateway</td>
<td>Enables users to place ISDN-to-IP or IP-to-IP calls through a gateway.</td>
<td>Y N N</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>Video Network &gt; IP Network &gt; Gatekeeper</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Gatekeeper</td>
<td>Specifies whether to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong> — Calls do not use a gatekeeper.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong> — System attempts to automatically find an available gatekeeper.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Specify</strong> — Calls use the specified gatekeeper. Enter the gatekeeper’s IP address or name (for example, gatekeeper.companyname.usa.com, or 10.11.12.13).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gatekeeper IP Address</td>
<td>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.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Use Gatekeeper for Multipoint Calls</td>
<td>Specify whether multipoint calls use the system’s internal multipoint capability or the Conference on Demand feature.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td><strong>Video Network &gt; IP Network &gt; Gateway Number</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country Code</td>
<td>Specifies the country code for the system’s location</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Area Code</td>
<td>Specifies the area or city code for the system’s location</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Gateway Number</td>
<td>Specifies the gateway’s number</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Gateway Number Type</td>
<td>Specifies the number type users enter to call this system:</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>• <strong>Direct Inward Dial</strong> — Users enter an internal extension to call this system directly.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you choose this setting, you must also register the number with the gatekeeper as an E.164 alias.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Number + Extension</strong> — Users enter the gateway number and the system’s extension to call this system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of digits in DID Number</td>
<td>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.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Number of digits in Extension</td>
<td>Specifies the number of digits in the extension used when Direct Inward Dial is selected. Your organization’s dial plan determines this number.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
Scheduled Endpoint Provisioning

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>
</table>
| Type of Service Field         | Specifies the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control:  
  • **IP Precedence** — Represents the priority of IP packets sent to the system. The value can be between 0 and 7.  
  • **DiffServ** — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field. | Y          | Y          | Y          |

| Video Type of Service Value   | 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. | Y          | Y          | Y          |

| Audio Type of Service Value   | Specifies the IP Precedence or Diffserv value for audio packets. | Y          | Y          | Y          |

| FECC Type of Service Value    | Specifies the IP Precedence or Diffserv value for Far End Camera Control packets | Y          | Y          | Y          |

| Enable Dynamic Bandwidth      | Specifies whether to let the system automatically find the optimum line speed for a call | Y          | Y          | N          |

| Enable PVEC                   | Enables the system to use PVEC (Polycom Video ErrorConcealment) if packet loss occurs. | Y          | Y          | Y          |

Video Network > IP Network > Firewall Settings

| Use Fixed Ports               | Specifies 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. | Y          | Y          | Y          |

| Start TCP Port                | 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.  
  **Note**  
  You must also open the firewall’s TCP port 1720 to allow H.323 traffic. | Y          | Y          | Y          |

Polycom, Inc. 266
### Scheduled Endpoint Provisioning

<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>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 NAT Public (WAN) Address.</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 <strong>Manual</strong>, 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>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>
</tbody>
</table>

#### Video Network > ISDN BRI Protocol

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ISDN H.320</td>
<td>Enables this system to make H.320 (ISDN) calls.</td>
<td>Y</td>
<td>Y</td>
<td>N</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>N</td>
</tr>
<tr>
<td>ISDN Switch Protocols</td>
<td>Specifies the protocol used by your network’s switch.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Outside Line Dialing Prefix</td>
<td>Specifies the ISDN dialing prefix used to call outside the network.</td>
<td>Y</td>
<td>Y</td>
<td>N</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>Video Network &gt; Preferred Speeds</strong></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 <strong>Call Quality</strong> selection is either unavailable or set to <strong>Auto</strong> on the <strong>Place a Call</strong> 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</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>International ISDN 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>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td><strong>Maximum Speed for Receiving Calls (Kbps)</strong></td>
<td>Restricts the bandwidth used when receiving IP or ISDN calls. 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>IP Calls</td>
<td></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>N</td>
</tr>
<tr>
<td><strong>Monitors &gt; Monitors 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Monitors</td>
<td>The number of monitors of QDX.</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Monitor 1 Options</strong></td>
<td></td>
<td></td>
<td></td>
<td></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>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Video Format</td>
<td>Specifies the monitor’s format: • DVI — Select if the monitor is connected to the DVI connector using a DVI or HDMI cable. • VGA — Select if the monitor is connected to the DVI connector using a VGA cable. • 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. • S-Video (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using an S-Video cable. • Composite (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using a composite video cable.</td>
<td>Y</td>
<td>Y</td>
<td>N</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>N</td>
<td>Y</td>
<td>N</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>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>N</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>N</td>
<td>Y</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>VGA Resolution of VSX.</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Monitor 2 Options</td>
<td>Applies to:</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Monitor 2</td>
<td>Specifies the second monitor's aspect ratio:</td>
<td>Y</td>
<td>N</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>Video Format</td>
<td>Specifies the monitor's format:</td>
<td>Y</td>
<td>N</td>
<td>Y</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>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>N</td>
<td>Y</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>People Display Mode</td>
<td></td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Content Display Mode</td>
<td></td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Color System</td>
<td></td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Monitor 3 Options

**Monitor 3**
Specifies the aspect ratio for recording.
- **Off** — Select if you do not have a VCR or DVD player connected to record video conferences.
- **4:3** — Select to record for playback on a standard monitor.
- **16:9** — Select to record for playback on a wide-screen monitor, if your recording device has this capability.

See the endpoint product documentation for more information about these selections.

**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.

**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.

**VCR/DVD Record Source**
Specifies the video source to be recorded to videotape or DVD.
- If **Near** is enabled, the recorded video will switch to the current near site speaker.
- If both **Near** and **Far** are enabled, the recorded video will switch between near and far sites depending on the current speaker.
- If **Content** is enabled, any content sent during the call is recorded.

**Screen Saver Wait Time**
The time the system will delay before going into standby mode after nonuse

### 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.

**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.

**Primary Camera**
Specifies which camera is the main camera.
<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>Camera Direction</td>
<td>Specifies the direction the camera moves when using the arrow buttons on the remote control.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Cameras &gt; Camera Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera 1 Name</td>
<td>Specifies a name for camera 1.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Camera 1 Icon</td>
<td>Specifies an icon for camera 1.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Camera 2 Name</td>
<td>Specifies a name for camera 2.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Camera 2 Icon</td>
<td>Specifies an icon for camera 2.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Camera 3 Name</td>
<td>Specifies a name for camera 3.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Camera 3 Icon</td>
<td>Specifies an icon for camera 3.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Cameras &gt; Video Quality</td>
<td>Specifies Motion or Sharpness for the video input. The default is Sharpness.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera 1</td>
<td>• <strong>Motion</strong> — This setting is for showing people or other video with motion.</td>
<td>Y</td>
<td>Y</td>
<td>Y</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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera 3</td>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Audio Settings &gt; Audio Settings 1</td>
<td>Sets the volume level of the ring tone and user alert tones.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Sound Effects Volume</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incoming Video Call</td>
<td>Specifies the ring tone used for incoming calls.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>User Alert Tones</td>
<td>Specifies the tone used for user alerts.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Mute Auto Answer Calls</td>
<td>Specifies whether to mute incoming calls.</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Line Input</td>
<td>Specifies the type of equipment that is connected to audio input 1.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Input Type Level</td>
<td>Sets the volume level for audio input 1.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Line Input Level</td>
<td>Sets the volume level for audio input 2.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
### Scheduled Endpoint Provisioning

<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 Outputs</td>
<td>Specifies how the audio output behaves. The default selection, <strong>Monitor - Far Site Audio</strong>, 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 <strong>Monitor - Far and Near Audio</strong> to supply audio from both the far site and the system’s microphones.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Line Output Level</td>
<td>Sets the volume level for audio output</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

**Audio Settings > Audio Settings 2**

<table>
<thead>
<tr>
<th>Field</th>
<th>Settings Description</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Audio Volume</td>
<td>Sets the volume level for audio from the far site.</td>
<td>Y</td>
<td>Y</td>
<td>Y</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>N</td>
<td>Y</td>
<td>N</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>N</td>
</tr>
<tr>
<td>Treble</td>
<td>Sets the volume level for the high frequencies without changing the master audio volume.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

**LAN Properties > LAN Properties 1**

<table>
<thead>
<tr>
<th>Field</th>
<th>Settings Description</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to My LAN</td>
<td>Enables connection to the local area network</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies how the system obtains an IP address.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>• <strong>Obtain IP Address Automatically</strong> — Select if the system gets an IP address from the DHCP server on the LAN.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enter IP Address Manually</strong> — Select if the IP address will not be assigned automatically.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Use the Following IP Address</td>
<td>If you selected <strong>Enter IP Address Manually</strong>, enter the IP address here.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

**LAN Properties > LAN Properties 2**

<table>
<thead>
<tr>
<th>Field</th>
<th>Settings Description</th>
<th>HDX Series</th>
<th>VSX Series</th>
<th>QDX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Servers</td>
<td>Displays the DNS servers currently assigned to the system.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>If the system does not automatically obtain a DNS server address, enter up to four DNS servers here.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>If the system does not automatically obtain a gateway IP address, enter one here.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Changing this setting causes the system to restart.</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>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 Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WINS Server</td>
<td>Displays the server running the Windows Internet Name Service</td>
<td>N Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WINS Resolution</td>
<td>Enables connection to the WINS Server for URL resolution</td>
<td>N Y</td>
<td></td>
<td></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.</td>
<td>Y Y Y</td>
<td></td>
<td></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.</td>
<td></td>
<td>Y Y Y</td>
<td></td>
</tr>
<tr>
<td>Global Services &gt; Directory Servers</td>
<td></td>
<td></td>
<td>Y Y Y</td>
<td></td>
</tr>
<tr>
<td>Global Directory (GDS)</td>
<td>Specifies the IP address or DNS address of the Global Directory Server.</td>
<td></td>
<td>Y Y Y</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Lets you enter the global directory password, if there is one.</td>
<td>Y Y Y</td>
<td></td>
<td></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>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Global Addresses</td>
<td>Displays other registered systems in the global directory.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Register</td>
<td>Registers this system with the Global Directory Server.</td>
<td>Y Y Y</td>
<td></td>
<td></td>
</tr>
<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>Y 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>Show Addresses in Address Book</td>
<td></td>
<td>N</td>
<td>N</td>
<td>N</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>N</td>
<td>N</td>
<td>N</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>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>International ISDN calls</td>
<td>• The call is placed from the directory</td>
<td>N</td>
<td>N</td>
<td>N</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>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

**LAN/H.323 > Global Directory (GDS) > Preferred Alias**

<table>
<thead>
<tr>
<th>Preferred Alias</th>
<th>Possible values include:</th>
<th>N</th>
<th>N</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td></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**

| Require Account Number to Dial           | Specify whether to require an account number for placing calls and whether that number should be validated by the system. | Y          | Y          | N          |
| Validate Account Number                  | Specify whether to require an account number for placing calls and whether that number should be validated by the system. | Y          | Y          | N          |

**Global Services > My Info**

| Contact Person                           | Specifies the name of the person responsible for this system | Y          | Y          | Y          |
| Contact Number                           | Specifies the phone number of the person responsible for this system | Y          | Y          | Y          |
| Contact e-mail                           | Specifies the e-mail address of the person responsible for this system | Y          | Y          | Y          |
| Contact Fax                              | Specifies the Fax number of the person responsible for this system | Y          | Y          | Y          |
| Tech Support                             | Specifies the contact information for Technical Support for this system | Y          | Y          | Y          |
| City                                     | Specifies the location of the person responsible for this system | Y          | Y          | Y          |
| State/Province                           |                                                       | Y          | Y          | Y          |
| Country                                  |                                                       | Y          | Y          | Y          |
Dynamic Management

When you dynamically manage an endpoint, you can remotely control the configuration settings and software version of the endpoint, according to policies you define.
Understanding Dynamic Endpoint Management

Administrators use the flexibility of a rule-based system to apply dynamic provisioning profiles. An administrator can create multiple rules and associate a profile with more than one rule at a time. A provisioning rule consists of one or more conditions that must be met before the dynamic provisioning profile can be applied.

Dynamic management enables a Polycom endpoint to poll the Polycom® RealPresence® Resource Manager system automatically to get provisioning updates (configuration settings) and software updates on a regular basis.

Dynamic management is client-to-server over HTTPS which makes it more secure and firewall-friendly.

Dynamic management is available:

- Only for Polycom endpoints.
- When Polycom endpoints are able to automatically discover the RealPresence Resource Manager system. This means you need to add the DNS service record (SRV record) for the RealPresence Resource Manager system to your DNS server.

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 either is found, the package URL 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.

Supported Polycom Endpoints and Peripherals

You can only dynamically manage some Polycom endpoints. The following Polycom endpoints and peripherals can be dynamically managed:

- RealPresence Group Series systems (must be dynamically managed)
- RealPresence Immersive Studio systems (must be dynamically managed)
- RealPresence Group Touch Control
- RealPresence Mobile (must be dynamically managed)
- RealPresence Desktop (must be dynamically managed)
- Polycom VVX systems
- Polycom HDX systems
- HDX Touch Control
- CMA Desktop (must be dynamically managed)
- Polycom CX5100
Overview of Dynamic Management Setup

Setting up dynamic management of Polycom endpoints is a multi-step process. You'll need to have your DNS server configured, the endpoint needs to be configured to use the RealPresence Resource Manager system as its provisioning server, and you need to set up provisioning profiles and software updates.

You need to dynamically provision a Polycom endpoint BEFORE you integrate with the RealPresence DMA system. If you manually register the system with the RealPresence DMA system before you dynamically provision the endpoint, the RealPresence Resource Manager system will show two endpoints in the Monitoring screen instead of one.

Configure Endpoints to use a Provisioning Service

You can configure the endpoint to use the RealPresence Resource Manager system as its provisioning service via the endpoint's web interface or soft endpoint's utility. You can do this on initial setup or at any time when you need to switch to dynamic management.

Some Polycom endpoints must be dynamically managed, such as RealPresence Desktop, RealPresence Mobile, RealPresence Group Series systems, and RealPresence Immersive Studio systems.

If you want to dynamically manage RealPresence Debut systems, you must use zero-touch provisioning. See Using Zero-Touch Provisioning for details.

Define Endpoint Naming Schemes

The RealPresence Resource Manager allows administrators to configure their E.164 alias, system naming schemes and SIP URIs for endpoints that are dynamically managed.

If you choose to provision H.323 settings through a network provisioning profile, you can also define the E.164 number and system naming scheme used for endpoints. You can also auto-generate SIP URIs for dynamically managed endpoints.

Create Video Endpoint Provisioning Profiles

Dynamic provisioning enables endpoints to poll the RealPresence Resource Manager automatically to get provisioning updates (configuration settings) on a dynamic basis. The provisioning profiles the endpoint receives are based provisioning rules you define.

When you dynamically manage endpoints (have the endpoint use the RealPresence Resource Manager as its provisioning server), you can automatically configure them by using provisioning profiles.

You need to modify and create three types of video endpoint provisioning profiles:

- **Network Provisioning** profiles define Network settings such as security, quality of service, and gatekeeper address, SIP server address, and so on.
● **Admin Config** Provisioning profiles define endpoint administrative settings such as maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on.

● **Bundled Provisioning** profiles allow you to control system settings that affect user experience.

**Create Provisioning Rules**

You can create rules that include conditions that need to be met before the RealPresence Resource Manager system sends a provisioning profile to an endpoint. You can also prioritize these rules so that certain provisioning profiles get applied first.

**Create Access Control Lists**

Access Control Lists provide an additional level of endpoint provisioning security when you dynamically manage endpoints. These lists allow you to group endpoints into “white lists” that can be dynamically provisioned. This is particularly useful when controlling Polycom’s soft endpoints such as CMA Desktop and RealPresence Mobile which use the provisioning credentials to authenticate with your video network. With Polycom RealPresence Mobile clients, you can also control access according to model (for example, RealPresence Mobile for the iPad).

**Create Software Updates**

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

**Selective Provisioning of Dynamically Managed RealPresence Group Series Systems**

By default, each setting within the provisioning profile that you use is provisioned to the endpoint. The settings within the profile overwrite any settings that were set locally for the endpoint. In addition, some settings become read-only on the endpoint.

However, when you dynamically manage a RealPresence Group Series system, you can choose to selectively provision fields within the provisioning profile. This means you can unmark fields within the profile that you do not want to set with the dynamic provisioning profile. For example, you may want the endpoint administrator to locally configure the language or time zone of the endpoint. Choosing this option does not affect other dynamically managed endpoints that may use the same profile.

**Dynamically Manage RealPresence Immersive Studio Systems**

A RealPresence Immersive Studio system contains multiple endpoints (codecs). When the RealPresence Resource Manager system dynamically manages (required) these devices, they display as a group of three codecs that follow a specific numbered naming convention that helps specify the total number of codecs included in the system. This is in addition to any system name you have configured. For example, the three RealPresence Group Series in an RealPresence Immersive Studio system named
wangle1PCTCDMAQAITP could display in the RealPresence Resource Manager system screens and reports with the following names:

- wangle1PCTCDMAQAITP_3_1
- wangle1PCTCDMAQAITP_3_2
- wangle1PCTCDMAQAITP_3_3

In the Endpoint > Monitor View screen, dynamically managed RealPresence Immersive Studio systems display as expandable icons.

The RealPresence Resource Manager system also provisions settings as applying to a single system. You can only provision the primary codec (the device designated as 1); the RealPresence Resource Manager system automatically propagates any changes to the other devices in the ITP system.
Dynamically Updating Endpoint and Peripheral Software

The Polycom RealPresence Resource Manager system’s 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: dynamic and scheduled. Dynamic and scheduled software update are exclusive endpoint management scenarios. Endpoints enabled for dynamic 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. A multi-tenancy environment only supports scheduled update.

Supported Endpoint Types for Dynamic Software Update

The dynamic software update feature is only available for these endpoint types:

- Polycom HDX system endpoints deployed in dynamic management mode
- Polycom RealPresence Group Series deployed in dynamic management mode
- Polycom RealPresence Immersive Studio systems
- Polycom CMA Desktop systems (Windows and Mac)
- RealPresence Desktop systems (Windows and Mac)
- Polycom VVX systems
- Polycom Touch Controls for both HDX and Group Series
- Polycom RealPresence Debut
- Polycom RealPresence Centro™
- Polycom RealPresence OTX® Studio
- Polycom CX5100
- Polycom Pano

Polycom provides default dynamic software update profiles for RealPresence Desktop clients. Default software update profiles are not available for other endpoint systems.
Software Update Considerations for RealPresence Desktop

When you upgrade RealPresence Desktop clients, Polycom recommends that you temporarily configure the RealPresence Resource Manager system to reclaim soft endpoint licenses in a very short time (one day). As soon as the client’s license is reclaimed and re-distributed, the RealPresence Resource Manager system can accurately track the upgraded endpoints.

When you upgrade the RealPresence Desktop and RealPresence Mobile clients, you may see erroneous endpoint reports in the RealPresence Resource Manager system that show duplicate RealPresence Desktop endpoints. In addition, these erroneous duplicate endpoints will each consume a RealPresence Desktop license.

After upgrading your RealPresence Desktop and RealPresence Mobile clients, you can reconfigure the license reclamation to the value you need. The default is 30 days.

Creating Dynamic Software Updates for Endpoints

To implement a dynamic software update, you must first create respective software updates for your endpoints.

List the Serial Numbers for the Endpoints to be Updated

You need to create a .txt file containing a list of the endpoint serial numbers to included in a software update key file.

Only users with the administrator role can create dynamic software updates.

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

1. Go to Endpoint > Dynamic Management > Upload Software Updates.
2. Select the endpoint type for which to get serial numbers.
3. Click Get Serial Numbers from the More menu.
   - The Endpoint Serial Number List lists the endpoints of the selected type and model that are eligible for software updates.
4. As needed, click Filter ⬇️ to customize the endpoint list.
5. Select the specific endpoints to be updated.
6. Click Get Serial Numbers from the More menu.
   - The serial number(s) appear in the text box on the page.
7. Create a .txt file containing the serial number(s).
Dynamically Updating Endpoint and Peripheral Software

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.

82071007E1DACD
82070407E010CD
82041804878B2
82040903E00FB0

b Save the `.txt` file.

c Return to the endpoint serial number list and click Close. The Software Updates list reappears.

8 Repeat steps 2 through 7 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.

9 Click Close. The Software Updates list reappears.

Endpoint Serial Number List

The Endpoint Serial Number List lists 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>
</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.

| Area         | (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. |

Download the Required Software Package

You need to download the required software update.
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 Polycom Support.
   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 Upgrade Activation Keys

You need to request software upgrade activation keys. And you can review your key history at Polycom Support.

To request upgrade activation keys:

1. Go to Polycom Support.

2. Log in or Register for An Account.


4. In the Software Upgrade Key Code section, click Retrieve Software KeyCode.

5. When upgrading a single endpoint:
   a. Enter the serial number of the endpoint to be updated into the Serial Number field of the Single Upgrade Key Code section.
   b. Enter the version number to which you are upgrading and click Retrieve.
   c. The key code is returned on the screen.
   d. Record the key code and create a .txt file with the Serial Number - Key Code combination to be updated.
   e. Close the Product Activation screens.

6. When updating multiple endpoints from a prepared .txt file (step a):
   a. In the Multiple Upgrade KeyCode section, click Add Attachment.
   b. Browse to the location of the .txt file you created and click Upload.
   c. A file containing the Serial Number - Key Code combinations will be emailed to the specified email account.
   d. When you receive the .txt file, save it to your local system.

Do not modify or rename the file that Polycom sends.
Dynamically Updating Endpoint and Peripheral Software

7 Close the **Product Activation** screens.

**Upload the Software Update for Dynamic Software Updates**

Polycom recommends you to do software updates using the split packages available on Polycom Support to reduce system resource consuming.

**To upload the software package and create an software update:**

1. Go to **Endpoint > Dynamic Management > Upload Software Updates**.
2. Select an endpoint type to update.
3. Click **Add** +.
4. If an activation key code is required to activate the software update:
   a. Select the **Update Requires Key** check box.
   b. In the **Software Update Key File** field, browse to the .txt key file (received in Request Upgrade Activation Keys).

Some endpoints may not support this option.

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.

After uploading a software image, you cannot view and update the key file anymore. To update the file, you need to re-upload the software.

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 image for the endpoint type and model type is created.

**Related Topics**

*Request Upgrade Activation Keys*

**Using Dynamic Software Updates**

Dynamic software updates, which controls the endpoint’s software version level, is tied to the endpoint type and the policy you define.

In dynamic management mode, when an endpoint starts up 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.
Dynamically Updating Endpoint and Peripheral Software

**Decide the Software Version**

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

All endpoints have a current version of software. You can automatically overwrite that current software with a different software version on all dynamically managed endpoint systems.

- **Version to Use**: After you change the **Version to Use** selection from the current value to the new version, the next time a dynamically managed endpoint polls the RealPresence Resource Manager system, the endpoint will detect that it has a different software version than the **Version to Use** selection. The endpoint will automatically download and install the identified software update package. Use this method to force users to use a specific software version. Until the **Version to Use** selection is enabled, the dynamic software update is not activated.

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.

- **Allow this Version or Newer**: If you also enable the **Allow this version or newer** selection, anytime you upload a newer version of software into a dynamic software update that update will be automatically installed on all dynamically managed endpoint systems.

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 system will send the software package with the highest version number to the endpoint.

To roll back a Polycom CMA Desktop or RealPresence 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 a dynamic software update policy for an endpoint type:

1. Go to **Endpoint > Dynamic Management > Upload Software Update**.
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 dynamic software update package, make that version the **Version to use** and select **Allow this version or newer**.
   - To require a specific version of dynamic software update package, make that version the **Version to use** and clear **Allow this version or newer**.
   - To turn off dynamic software update for an endpoint type, change the **Version to use** value to **(none)**.
4. Click **Update**.
**View Dynamic Software Update Status**

You can view the list of endpoints that have registered to the system for dynamic software updates.

To view the list of endpoints registered to the system for dynamic updates:

1. Navigate to **Endpoint > Dynamic Management > Software Update Status** menu to view the list of endpoints that have registered to the system for dynamic software updates.

2. Click **Filter** to use for the list. Filter choices for this view include:
   - **Endpoint Type**—Filters the list by endpoint type.
   - **Endpoint 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.

3. Use the **Items per page** drop-down to customize the number of endpoints included per page.

**Endpoint List for Dynamic Software Updates**

The endpoint list includes the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the endpoint’s last software update. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Success</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Clear</td>
</tr>
<tr>
<td></td>
<td>• Timed Out</td>
</tr>
<tr>
<td></td>
<td>• Skipped (only applied to CMA Desktop and RealPresence Desktop clients)</td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>The system name of the endpoint.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of endpoint. Dynamic software update is only available for these</td>
</tr>
<tr>
<td></td>
<td>endpoint types:</td>
</tr>
<tr>
<td></td>
<td>• HDX systems (when dynamically managed)</td>
</tr>
<tr>
<td></td>
<td>• RealPresence Group Series (when dynamically managed)</td>
</tr>
<tr>
<td></td>
<td>• RealPresence Immersive Studio systems (when dynamically managed)</td>
</tr>
<tr>
<td></td>
<td>• CMA Desktop</td>
</tr>
<tr>
<td></td>
<td>• RealPresence Desktop</td>
</tr>
<tr>
<td></td>
<td>• Polycom VVX</td>
</tr>
<tr>
<td></td>
<td>• Polycom CX5100</td>
</tr>
<tr>
<td></td>
<td>• Polycom Pano</td>
</tr>
</tbody>
</table>
Dynamically Updating Endpoint and Peripheral Software

Users with the Device Administrator, Administrator or the Area Administrator role can view details about dynamic software updates made to endpoints.

To view detailed information for endpoints that are eligible for dynamic software updates:

1. Go to **Endpoint > Dynamic Management > Software Update Status**.
2. As needed, click **Filter** to customize the endpoint list. Filter choices include **Endpoint Type**, **Endpoint Name**, **IP Address**, **ISDN Video Number**, **Dial String**, **Site** and **Area**.
3. Select the endpoint of interest.
4. Click **View Details** and expand the **Software Update Details** section to view the details for the endpoint.

**Related Topics**

Dynamic Software Details
View Software Update Details

**Dynamic Software Details**

The endpoint list in the **Dynamic Software Details** pane has the following information.
### Field | Description
--- | ---
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.

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.

**Note**
Polycom CMA Desktop systems and RealPresence Desktop clients are updated at the start of each session.

### Field | Description
--- | ---
Scheduled | For dynamic 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.

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.

---

**View Dynamic Software Update Packages**

You can view a list of software updates available to dynamically managed endpoints and the update policies.
To view the list of dynamic software update packages:

1. Go to Endpoint > Dynamic Management > Upload Software Update.

   The Dynamic Software Policies page appears and the uploaded software update packages are displayed.

2. To view the dynamic software update packages for other endpoints and peripherals, select the appropriate item from the Device Type drop-down list: HDX, Group Series, CMA Desktop (PC or Mac OS), VVX or HDX Touch Control, Group Series Touch Control, and RealPresence Desktop (PC or Mac OS).

Dynamic Software Updates

The Dynamic Software Updates page includes this information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Area</td>
<td>Enables you to specify an area to which to apply the update. This option is only available when areas are enabled and for areas that the user is allowed to manage.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>The type of endpoint system. You can use dynamic software updates for the supported Polycom endpoints and peripherals.</td>
</tr>
<tr>
<td>Version to use</td>
<td>Displays the default dynamic 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 dynamic 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 dynamic software update package.</td>
</tr>
<tr>
<td>Description</td>
<td>The meaningful name given to the dynamic software update package when it was created.</td>
</tr>
<tr>
<td>Uploaded</td>
<td>The date and time when the dynamic 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>

Set Maintenance Window for Dynamic Software Updates

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

This feature only applies to dynamically managed HDX and RealPresence Group Series.

Typically, dynamic software updates occur as specified by the Software Update Polling Interval that is provisioned with the network provisioning profile for the endpoint.
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 endpoints, and the endpoints hold their dynamic software update requests until the maintenance window starts.

To avoid dynamically updating the software on all HDX or RealPresence Group Series at the start of the maintenance window, the systems randomize their dynamic software update requests.

To restrict dynamic software updates to a scheduled maintenance window:

1. Go to Endpoint Management > Dynamic Management > Upload Software Update.
2. Select the appropriate device type: HDX or Group Series.
3. Click Maintenance Window from the More menu.
4. In the Maintenance Window dialog, 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 endpoint’s 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.
5. Click OK.

Set up a Trial Dynamic Software Update

Set up a trial user group for trial software update. After you create a software update, you can set up a trial of a software update.

Users with the administrator role can do this.

To trial a software update package:

1. Creating a Local Trial Group.
2. Create a Trial Software Update Package.

Related Topics

Creating Dynamic Software Updates for Endpoints
Promote the Trial Software Update Package to Production
Delete the Trial Software Update Package.

Creating 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. The people in this group will receive the trial software update package when their endpoint goes through its normal, automated software update process.
Dynamically Updating Endpoint and Peripheral Software

- 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.

Related Topics
Add a Local Group

Create a Trial Software Update Package
You need to upload the software packages before you create a trial software update package.

To create a trial dynamic software update package:

1. 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 Creating a Local Trial Group.
2. Click OK.
   A trial dynamic software update package for the endpoint type and model type appears in the Dynamic 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.

Related Topics
Creating a Local Trial Group

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 Endpoint > Dynamic Management > Upload Software Updates.
2. Select the endpoint type 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 dynamic 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 Endpoint > Dynamic Management > Upload Software Updates.
2. Select the endpoint type to update.
3. Select the software update package you want to delete and click Delete.
4. Click Yes to confirm the deletion.
   The package is removed from the Dynamic 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 dynamic software update policy.

Related Topics

Decide the Software Version

Populate Domain Name for Software Endpoints

If you use only one domain, you can set the domain name in the RealPresence Resource Manager, which will automatically populate the domain name for your software endpoints.

To set the domain name:
1. Go to Endpoint > Dynamic Management > Endpoint Management Settings > Default Domain Name Setting.
2. Select the check box of Set the default domain name for Enterprise user login from software endpoint.
3. In the Default Domain Name box, specify the domain name.
4. Click Update.

Enable Software Endpoints to Save Password

You can make the software endpoints save the passwords with the help of a provisioning attribute. Both RealPresence Mobile endpoints and RealPresence Desktop endpoints support the setting.

By default, the setting is disabled.

To save the password:
1. Go to Endpoint > Dynamic Management > Endpoint Management Settings > Remember Password Options.
2 Select the check box of Enable “Remember Password” for the software endpoints.
3 Click Update.

Dynamic 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 more 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 Polycom Support and make them available from the RealPresence Resource Manager system web server. You can also configure which updates are for trial or production use.

View Software Updates for Polycom Touch Controls

You can view a list of the software updates available for Polycom Touch Controls. This includes status information, the software version, and so on.

**To view software updates for peripherals:**

1 Go to Endpoint > Dynamic Management > Upload Software Updates.
2 Select the HDX Touch Control or Group Series Touch Control tab to view the information.

Peripheral Software Updates

The HDX Touch Control or Group Series Touch Control tab includes this information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Area</td>
<td>Enables 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>
</tbody>
</table>
Dynamically Updating Endpoint and Peripheral Software

### Upload Peripheral Software Updates to the RealPresence Resource Manager System

After you download the software updates from Polycom Support and save them on your hard drive, you can upload them to the RealPresence Resource Manager system.

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

1. Go to Endpoint > Dynamic Management > Upload Software Updates.
2. Select the endpoint type for the peripheral.
3. Click Add.
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

You need to configure software updates for peripherals to be used in production.

**To configure software updates for production:**

1. Go to Endpoint > Dynamic Management > Upload Software Updates.
2. Select the RealPresence Touch, HDX Touch Control, or Group Series Touch Control as the peripheral endpoint type.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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</td>
</tr>
<tr>
<td></td>
<td>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>

*Production URL*

*Trial URL*
3 Click More > Configure Production to configure the peripheral updates.

4 Click OK.

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

Configuring Production Settings

The Configure Production 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Configure Application</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<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. 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.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the application 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>
</tbody>
</table>
Configure Peripheral Updates for Trial

You need to configure the software updates to be used for the trial.

To configure software updates for trial:
1. Go to Endpoint > Dynamic Management > Upload Software Updates.
2. Select the endpoint type for the peripheral.
3. Click More > Configure Trial to configure the peripheral updates for trial.
4. 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.

Configuring Trial Settings

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>
</tbody>
</table>
### Field | Description
--- | ---
Platform Compatible | 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.

### 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.
Using Dynamic Provisioning Profiles

The Polycom RealPresence Resource Manager system enables you to use provisioning profiles and provisioning rules as a way to dynamically manage endpoint settings.

If your deployment includes a RealPresence Access Director system that you want to dynamically manage, you can create a RealPresence Access Director Server Provisioning Profile.

Set up Dynamic Provisioning Profiles

When you dynamically manage endpoints (have the endpoint use the RealPresence Resource Manager as its provisioning server), you can automatically configure them by using provisioning profiles.

Dynamic provisioning profiles are applied through a rule-based paradigm.

Dynamic provisioning consists of following steps:

1. Create a dynamic provisioning profile.
2. Create one or more provisioning rules.
3. Associate a provisioning profile with a rule.

Types of Dynamic Endpoint Provisioning Profiles

The RealPresence Resource Manager provides three types of provisioning profiles for use when you dynamically manage endpoints.

<table>
<thead>
<tr>
<th>Dynamic Provisioning Profile</th>
<th>Summary of Provisioned Settings:</th>
<th>How applied:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network provisioning profile</td>
<td>Defines network settings such as security, quality of service, and gatekeeper address, SIP server address, and so on.</td>
<td>Applied according to the provisioning rules you define.</td>
</tr>
</tbody>
</table>
Using Dynamic Provisioning Profiles

Provisioning profiles contain parameters that apply to endpoints.

**Working with Provisioning Profiles**

Navigate to **Endpoint > Dynamic Management > Provisioning Profiles** to work with both Network and Admin Config provisioning profiles.

**Create a New Provisioning Profile**

As soon as an endpoint is configured to use the RealPresence Resource Manager for its provisioning server, it starts polling for provisioning profile updates. So to ensure out-of-box usability, the RealPresence RealPresence Resource Manager system comes with a default provisioning profiles. These default profiles cannot be customized with any rule but apply to all video endpoints by default.

You need to create new provisioning profiles to customize endpoint settings in your environment. New provisioning profiles are based on the default profiles. Any changes you make to the default profiles are not applied to pre-existing profiles.

Not all of the provisioning parameters apply to all endpoint systems being provisioned. If an endpoint system does not have a corresponding parameter, it ignores the parameter.

**To create a provisioning profile:**

1. Go to **Endpoint > Dynamic Management > Provisioning Profiles**.
2. Click +.
3. In the **General Info** section of the **Add New Profile** section, enter a name for the new provisioning profile.
4. Select a provisioning profile type from the drop-down list.

<table>
<thead>
<tr>
<th>Dynamic Provisioning Profile</th>
<th>Summary of Provisioned Settings:</th>
<th>How applied:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Config provisioning profile</td>
<td>Defines endpoint administrative settings such as maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on.</td>
<td>Applied according to the provisioning rules you define.</td>
</tr>
<tr>
<td>Bundled provisioning profile</td>
<td>Allows you to configure endpoint system settings according to endpoint model and software version. Home screen settings related to user experience, monitor display and camera settings, password format settings and so on.</td>
<td>Applied according to model and software version of the particular endpoint.</td>
</tr>
</tbody>
</table>
5 If the profile will be used for RealPresence Group systems, mark the **Selectable Provisioning for Group Series** check box.  
   When this check box is marked, the RealPresence Group systems that use this profile will only be provisioned with the settings you select. You can select settings by marking the respective check box next to the setting.

6 As needed, edit the provisioning details.

7 Click **OK**.

**Related Topics**

- Available Settings for a Network Provisioning Profile
- Available Settings for Admin Config Provisioning Profiles

**Edit a Provisioning Profile**

You can edit a provisioning profile.

To edit a provisioning profile:

1 Go to **Endpoint > Dynamic Management > Provisioning Profiles**.
2 In the **Provisioning Profiles** page, select a profile and click **Edit**.
3 If the profile will be used for RealPresence Group systems, mark the **Selectable Provisioning for Group Series** check box.  
   When this check box is marked, the RealPresence Group systems that use this profile will only be provisioned with the settings you select. You can select settings by marking the respective check box next to the setting.
4 As needed, edit the provisioning details.
5 Click **OK**.  
   The provisioning profile is updated.

**Reset a Provisioning Profile**

When you reset a provisioning profile, you reset the values of this profile to the default values of its profile type. For example, profile_A is a **Network Provisioning Profile**. After you reset profile_A, the parameter values of profile_A will be the same as the default **Network Provisioning Profile** that comes with the system.

To reset a default provisioning profile:

1 Navigate to **Endpoint > Dynamic Management > Provisioning Profiles**.
2 In the **Provisioning Profiles** page, select a profile and click **Reset**.  
   You cannot change the name of the selected provisioning profile.
3 Click **OK**.
**Edit a Default Provisioning Profile**

You can edit a default provisioning profile.

To edit a default provisioning profile:

1. Go to **Endpoint > Dynamic Management > Provisioning Profiles**.
2. In the **Provisioning Profiles** page, select a default profile and click **Edit**.
   
   You may find more implementation details about these fields in the respective system documentation.

3. If the profile will be used for RealPresence Group systems, mark the **Selectable Provisioning for Group Series** check box.
   
   When this check box is marked, the RealPresence Group systems that use this profile will only be provisioned with the settings you select. You can select settings by marking the respective check box next to the setting.

4. Click **OK**.

**Reset a Provisioning Profile**

You can reset a provisioning profile you created. When you reset a provisioning profile, its values revert to the values derived from the default template of the same type.

To reset a provisioning profile:

1. Go to **Endpoint > Dynamic Management > Provisioning Profiles**.
2. In the **Provisioning Profiles** page, select a default profile and click **Reset**.
   
   You may find more implementation details about these fields in the endpoint system documentation.

3. Click **OK**.
   
   The default provisioning profile is updated.

**Clone a Provisioning Profile**

You can clone a provisioning profile. This enables you to re-name an existing profile.

To clone a provisioning profile:

1. Go to **Endpoint > Dynamic Management > Provisioning Profiles**.
2. In the **Provisioning Profiles** page, select the profile of interest and click **Clone**.
3. In the **Clone Profile** dialog, enter a name for the new profile and click **Save**.
   
   The provisioning profile appears last in the Provisioning Profiles list.

4. As needed, edit the profile.
Delete a Provisioning Profile

You can delete a provisioning profile.

To delete a provisioning profile:
1. Go to Endpoint > Dynamic Management > Provisioning Profiles.
2. In the 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.

Network Provisioning Profiles

With network provisioning profiles, you can ensure that all dynamically managed endpoints have the optimal and correct settings respective to their network location.

Network provisioning profiles allow you to provision endpoints with network settings such as security, quality of service, gatekeeper address, SIP server address, and so on.

You need to create new network provisioning profiles to have rule-based network settings in your video environment.

Available Settings for a Network Provisioning Profile

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Profile Name</td>
<td>Specify a unique name for the profile</td>
</tr>
<tr>
<td>Provisioning Profile Type</td>
<td>Choose the profile type from the drop-down list.</td>
</tr>
<tr>
<td>Selectable Provisioning for Group Series</td>
<td>When you mark this check box, you can manually select which settings within the provisioning profile are sent to a RealPresence Group Series system. Only the selected settings will be provisioned to RealPresence Group Series systems. Within the provisioning profile, only the settings that you select are set to the RealPresence Group Series system. For example, if a provisioning setting is blank but still checked, the blank value is still be provisioned to the system. By default, all settings are checked. If you don’t want to provision the setting to the RealPresence Group Series system, you must uncheck the individual settings.</td>
</tr>
<tr>
<td><strong>Date and Time Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Specify the country code for their location.</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>
</tbody>
</table>
### Using Dynamic Provisioning Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Format</td>
<td>Specify the time display format.</td>
</tr>
<tr>
<td>Time Server</td>
<td>Specify whether to connect to a time server for automatic system time settings. Select <strong>Auto</strong> 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 <strong>Manual</strong> 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 <strong>Time Server Address</strong> field. If <strong>Time Server</strong> is set to <strong>Off</strong>, or if the <strong>Time Server</strong> is set to <strong>Manual</strong> or <strong>Auto</strong> but the endpoint system cannot connect to the time server, the date and time must be manually reset at the endpoint.</td>
</tr>
<tr>
<td>Primary Time Server Address</td>
<td>Specify the address of the primary time server when <strong>Time Server</strong> is set to <strong>Manual</strong>.</td>
</tr>
<tr>
<td>Secondary Time Server Address</td>
<td>Specify the address of the secondary time server when <strong>Time Server</strong> is set to <strong>Manual</strong>.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Specify the time difference between GMT (Greenwich Mean Time) and the endpoint system’s location.</td>
</tr>
<tr>
<td>Firewall Settings</td>
<td></td>
</tr>
<tr>
<td>Use Fixed Ports</td>
<td>Specify whether to define the TCP and UDP ports.</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>
</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>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></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>
</tr>
<tr>
<td>Start TCP Port</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>You must also open the firewall’s TCP port 1720 to allow H.323 traffic.</td>
</tr>
<tr>
<td>Start UDP Port</td>
<td>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.</td>
</tr>
<tr>
<td>Enable H.460 Firewall Traversal</td>
<td>Enables the endpoint system to use H.460-based firewall traversal. For more information, see the <em>Administrator’s Guide for Polycom HDX Systems</em>.</td>
</tr>
</tbody>
</table>

**Polycom, Inc.**
### Field | For the endpoint systems being provisioned...
--- | ---
NAT Configuration | Specify whether the endpoint systems should determine the NAT Public WAN Address automatically.  
- If the endpoint systems are behind a NAT that allows HTTP traffic, select Auto.  
- If the endpoint systems are behind a NAT that does not allow HTTP traffic, select Manual. Then specify a NAT Public (WAN) Address.  
- If the endpoint systems are not behind a NAT or are connected to the IP network through a virtual private network (VPN), select Off.

NAT Public (WAN) Address | When NAT Configuration is set to Manual, specify the address that callers from outside the LAN should use to call the endpoint systems.

NAT is H.323 Compatible | Specify that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.

Address Displayed in Global Directory | Specify whether to include the endpoint system’s information in the global directory  
- Select Private to exclude the endpoint from the global directory  
- Select Public to include the endpoint in the global directory

Enable SIP Keep Alives | When checked, SIP Keep Alive messages are enabled.

**H323 Settings**

Enable IP H.323 | Specify whether to enable IP H.323 calls.

Use Gatekeeper | Select one of the following items:  
- Off: Do not use a gatekeeper.  
- Auto: The RealPresence Resource Manager system finds an available gatekeeper automatically.  
- Specify: Specify the gatekeeper IP address in the Gatekeeper Address field.

Gatekeeper Address | When Use Gatekeeper is set to Specify, enter the gatekeeper address.

**Notes for endpoints that will use a RealPresence Access Director system or Polycom VBP**

If this network provisioning profile is used for endpoints within a site that includes a RealPresence Access Director system or Polycom VBP system, the gatekeeper IP address should be the external or subscriber IP address of the RealPresence Access Director or Polycom VBP system.

Use Gatekeeper for Multipoint Calls | 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.

**SIP Settings**

Enable SIP | Specify whether to enable SIP calls and enable the provisioning of SIP settings.

Automatically Discover SIP Servers | The RealPresence Resource Manager system sends provisioning info telling endpoints to auto discover SIP servers. The endpoint then performs a DNS query to locate the SIP server.
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server</td>
<td>Specify the IP address or FQDN of the SIP proxy server for the network. If you leave this field blank, the registrar server is used.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes for endpoints that will use a RealPresence Access Director system</strong></td>
</tr>
<tr>
<td></td>
<td>If this network provisioning profile is used for endpoints within a site that includes a RealPresence Access Director system, the Proxy Server IP address should be the external or subscriber IP address of the RealPresence Access Director.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Specify the IP address or FQDN 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 FQDN 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></td>
<td><strong>Notes for endpoints that will use a RealPresence Access Director system</strong></td>
</tr>
<tr>
<td></td>
<td>If this network provisioning profile is used for endpoints within a site that includes a RealPresence Access Director system, the Registrar Server address should be the external or subscriber IP address of the RealPresence Access Director.</td>
</tr>
<tr>
<td>Backup Proxy Server</td>
<td>Specify the IP address or FQDN of a backup SIP proxy server for the network.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes for endpoints that will use a RealPresence Access Director system</strong></td>
</tr>
<tr>
<td></td>
<td>If this network provisioning profile is used for endpoints within a site that includes a RealPresence Access Director system, the Backup Proxy Server IP address should be the IP address of the RealPresence Access Director.</td>
</tr>
<tr>
<td>Backup Registrar Server</td>
<td>Specify the IP address or FQDN of a backup SIP registrar server for the network.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes for endpoints that will use a RealPresence Access Director system</strong></td>
</tr>
<tr>
<td></td>
<td>If this network provisioning profile is used for a site that includes a RealPresence Access Director system, the Backup Registrar Server IP address should be the IP address of the RealPresence Access Director.</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></td>
<td>• Auto enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments.</td>
</tr>
<tr>
<td></td>
<td>• TCP provides reliable transport via TCP for SIP signaling.</td>
</tr>
<tr>
<td></td>
<td>• UDP provides best-effort transport via UDP for SIP signaling.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
</tbody>
</table>
Using Dynamic Provisioning Profiles

### Field | For the endpoint systems being provisioned...
--- | ---
Server Type | Specify the type of the SIP registrar server. You can provision the following SIP registrar servers:
- Standard (Polycom DMA system)
- Polycom
- 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 Endpoint Provisioning Credentials | Enable this option when the endpoint system should use the credentials the user entered at the endpoint for authenticating when registering with a SIP registrar server.

Use Enterprise URI | Enable this option when the endpoint system should use the SIP URI of the enterprise user (domain user).

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 credentials (username and password) can be used when the SIP server does not require unique user credentials.

Common SIP Password | Specify the password that authenticates the system to the registrar server. Common SIP credentials (username and password) can be used when the SIP server does not require unique user credentials.

### Provisioning Settings

Provisioning Polling Interval (minutes) | Specify the frequency at which the endpoint systems poll the RealPresence 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.

Software Update Polling Interval (minutes) | Specify the frequency at which the endpoint systems poll the RealPresence 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.

Enable Pano Updates via HTTP | Enable HTTP transfer for Pano software updates. This option is disabled by default. If disable this option, HTTPS transfer will be used for Pano updates. In this case, you need to install an official certificate to allow HTTPS connection for Pano updates.

### Quality of Service Settings

Video Type of Service Value | Specify the IP Precedence or Diffserv value for video packets.
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Type of Service Value</td>
<td>Specify the IP Precedence or Diffserv value for audio packets.</td>
</tr>
<tr>
<td>FECC Type of Service Value</td>
<td>Specify the IP Precedence or Diffserv value for Far End Camera Control packets.</td>
</tr>
</tbody>
</table>
| Type of Service Field                     | Specify the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control:  
  • **IP Precedence** — Represents the priority of IP packets sent to the system. The value can be between 0 and 5.  
  • **DiffServ** — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field. |
| Maximum Transmission Unit Size (bytes)    | 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. |
| Enable PVEC                               | Enables 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 |
| Enable RSVP                               | Enables 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. |
| Enable Dynamic Bandwidth                  | Specify whether to let the endpoint system automatically find the optimum line speed for a call. |
| Maximum Transmit Bandwidth (Kbps)         | Specify the maximum transmission line speed. |
| Maximum Receive Bandwidth (Kbps)          | Specify the maximum reception line speed. |
| Operation and Management Type             | Specifies the IP Precedence or Diffserv value for traffic not related to video, audio, or FECC. |

**Security Settings**

<p>| Security Profile                          | Read-only field. Displays the security level of the endpoint. |
| Enable Dynamic Provisioning for ID/Passwords | This check box must be marked if you want to provision IDs or passwords. |
| Enable Provisioning for Room Password     | Enable or disable room password provisioning. |
| Use Room Password for Remote Access       | Specify whether the local endpoint system password and remote access password are the same. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<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</td>
</tr>
<tr>
<td></td>
<td>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>Remote Access Password</td>
<td>For endpoint systems, enter or change the remote access password here. When the remote access password is set,</td>
</tr>
<tr>
<td></td>
<td>you must enter it to upgrade the software or manage the endpoint systems from a computer. The remote access</td>
</tr>
<tr>
<td></td>
<td>password cannot include spaces.</td>
</tr>
<tr>
<td>Meeting Password</td>
<td>Specify the password users must supply to join multipoint calls on this endpoint system if the call uses the</td>
</tr>
<tr>
<td></td>
<td>internal multipoint option, rather than a bridge. This field can also be used to store a password required by</td>
</tr>
<tr>
<td></td>
<td>another endpoint system that this system calls. If a password is stored in this field, you do not need to enter</td>
</tr>
<tr>
<td></td>
<td>it at the time of the call; the endpoint system supplies it to the system that requires it. The meeting password</td>
</tr>
<tr>
<td></td>
<td>cannot include spaces.</td>
</tr>
<tr>
<td>Enable Secure Mode</td>
<td>Specify whether to operate in secure mode (also known as security mode), which uses TLS, HTTPS, AES, digital</td>
</tr>
<tr>
<td></td>
<td>signatures, and other security protocols, algorithms, and mechanisms. These protocols encrypt management</td>
</tr>
<tr>
<td></td>
<td>communication over IP, preventing access by unauthorized users.</td>
</tr>
<tr>
<td></td>
<td>When devices at a site are provisioned to operate in secure mode, the RealPresence Resource Manager system can</td>
</tr>
<tr>
<td></td>
<td>only perform the dynamic management operations of automatic provisioning, automatic software update, and</td>
</tr>
<tr>
<td></td>
<td>directory and presence services for the devices. The RealPresence Resource Manager system cannot perform</td>
</tr>
<tr>
<td></td>
<td>monitoring or control operations for the devices.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Administrator’s Guide for Polycom HDX Systems.</td>
</tr>
<tr>
<td>AES Encryption</td>
<td>Specify how to encrypt calls with other sites that support AES encryption.</td>
</tr>
<tr>
<td></td>
<td>• Off—No encryption is used.</td>
</tr>
<tr>
<td></td>
<td>• When Available—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the</td>
</tr>
<tr>
<td></td>
<td>call don’t support it.</td>
</tr>
<tr>
<td></td>
<td>• Required for Video Calls Only—AES Encryption is used for all video endpoints in the call. Analog phone and</td>
</tr>
<tr>
<td></td>
<td>voice over ISDN connections are allowed. Video endpoints must support AES Encryption to participate in the</td>
</tr>
<tr>
<td></td>
<td>call.</td>
</tr>
<tr>
<td></td>
<td>• Required for All Calls—AES Encryption is used for all video endpoints in the call. Analog phone and voice</td>
</tr>
<tr>
<td></td>
<td>over ISDN connections are not allowed. All endpoints must support AES Encryption to participate in the call.</td>
</tr>
<tr>
<td>Enable Web Access</td>
<td>Specify whether to allow remote access to the endpoint system by the web.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate</td>
</tr>
<tr>
<td></td>
<td>the associated port, only the application. Use the <strong>Web Access Port</strong> setting to disable the port.</td>
</tr>
<tr>
<td>Enable HTTPS only</td>
<td>Select this check box to allow the endpoint to connect only using HTTPS.</td>
</tr>
</tbody>
</table>
### Using Dynamic Provisioning Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Telnet Access</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>Web Access Port</td>
<td>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. <strong>Note</strong> The system restarts if you change the web access port. This port setting only works for HTTP port.</td>
</tr>
<tr>
<td>Allow Video Display On Web</td>
<td>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. <strong>Note</strong> This feature activates both near site and far site video displays in Web Director.</td>
</tr>
<tr>
<td>NTLM Version</td>
<td>Specify the NTLM version the endpoint system should use to authenticate.</td>
</tr>
</tbody>
</table>

### Security Settings 2

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</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>
<tr>
<td>Enable NIDS</td>
<td>Enable Network Intrusion Detection messages.</td>
</tr>
<tr>
<td>FIPS 140 Mode</td>
<td>Support FIPS 140.</td>
</tr>
</tbody>
</table>
### Using Dynamic Provisioning Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Security Classification</td>
<td>Helps RealPresence Group system call participants remain conscious of the security classification when in a BroadWorks managed call.</td>
</tr>
<tr>
<td><strong>Whitelist</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Whitelist of IPs</td>
<td>When a white list is enabled, enables 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>
| 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 10.11.1.*.* to allow all IP addresses that begin with 10.11.                                                                 |
<p>| <strong>General Settings</strong>                 |                                                                                                                                                                                                                                            |
| Heartbeat Posting Interval (minutes) | Specify the frequency at which the endpoint systems poll the RealPresence Resource Manager system for a heartbeat.                                                                                                                            |
| In Call Stats Posting Interval (minutes) | Specify the frequency at which the endpoint systems poll the RealPresence Resource Manager system for in call statistics.                                                                                                             |
| <strong>Calendaring Settings</strong>             |                                                                                                                                                                                                                                            |
| Automatically Discover Exchange Server | Specify that the RealPresence Resource Manager system should discover the Microsoft Exchange server for the site by searching DNS records. If you have configured a Calendar Connector, you should use the Specify Exchange Server field instead. |
| Specify Exchange Server              | Specify that the RealPresence Resource Manager system should use the Microsoft Exchange server specified in the Exchange Server Address field.                                                                                           |
| Exchange Server Address              | Specify the IP address or FQDN of the Microsoft Exchange server for the site. If you have configured a Calendar Connector, put the RealPresence Resource Manager system FQDN in this field. See Calendar Connector for additional information.                      |
| <strong>Enterprise Directory Settings</strong>    |                                                                                                                                                                                                                                            |
| Group Display Name                   | Specify whether the RealPresence 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 RealPresence Resource Manager system should identify users by their common name (cn) or their DisplayName. These names are extracted from the Active Directory.                                                            |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Directory Admin Group</td>
<td>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.</td>
</tr>
<tr>
<td>Enterprise Directory User Group</td>
<td>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.</td>
</tr>
<tr>
<td>Use Default Authentication Server</td>
<td>This check box is only available if you have marked the Enterprise Directory Admin Group or the Enterprise Directory User Group. When checked, endpoints will use the RealPresence Resource Manager system’s IP address as the IP for the authentication server. If you have marked the Enterprise Directory Admin Group or the Enterprise Directory User Group and leave this check box unchecked, you must indicate an authentication server for provisioned endpoints.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>This check box is only available if you have marked the Enterprise Directory Admin Group or the Enterprise Directory User Group. If you have marked the Enterprise Directory Admin Group or the Enterprise Directory User Group and have NOT marked the <strong>Use Default Authentication Server</strong> check box, you must indicate an authentication server for provisioned endpoints.</td>
</tr>
</tbody>
</table>

### Directory Settings

- **Provision directory service for hardware endpoints**
  - Specifies that directory services will be enabled for all endpoints, including hardware endpoints. If unchecked, directory services are only provisioned to software endpoints.
- **Use Default Directory Server**
  - Use the RealPresence Resource Manager system to provide the directory service.
- **Directory Server**
  - When the **Use Default Directory Server** radio button is unchecked, you can use the **Directory Server** field enter the IP address of the directory server you wish to use.
- **Verify Certificate**
  - Enable this option when the endpoint system’s certificate should be verified by the certificate authority.

### Presence Settings

- **Use Default Presence Server**
  - Use the RealPresence Resource Manager system to provide the presence service.
- **Presence Server**
  - When the **Use Default Presence Server** button is unchecked, you can use the **Presence Server** field enter the IP address of the presence server you wish to use.
- **Verify Certificate**
  - Enable this option when the endpoint system’s certificate should be verified by the certificate authority.

### SNMP Settings

- **Enable SNMP Access**
  - Specify whether to allow remote access to the system by SNMP.

**Note**

The endpoint will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application.
<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Version1</td>
<td>Select to enable SNMP Version1.</td>
</tr>
<tr>
<td>SNMP Version2C</td>
<td>Select to enable SNMP Version2C.</td>
</tr>
<tr>
<td>SNMP Version3</td>
<td>Select to enable SNMP Version3.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Select TCP or UDP.</td>
</tr>
<tr>
<td>Listening Port</td>
<td>The default port is 161.</td>
</tr>
<tr>
<td>Read-only 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. The RealPresence RealPresence Resource Manager system has only one valid context—by default, public—which is identified by this Community name. The RealPresence RealPresence Resource Manager system will not respond to requests.</td>
</tr>
<tr>
<td>Contact Name</td>
<td>Specifies the name of the person responsible for remote management of this system.</td>
</tr>
<tr>
<td>Location Name</td>
<td>Specifies the location of the system.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the SNMPv3 User Security Model (USM) account name that will be used for SNMPv3 message transactions. The maximum length is 64 characters.</td>
</tr>
<tr>
<td>Auth Algorithm</td>
<td>Specifies the type of SNMPv3 authentication algorithm used:</td>
</tr>
<tr>
<td></td>
<td>• SHA</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td>Auth Password</td>
<td>Specifies the SNMPv3 authentication password. The maximum length is 48 characters.</td>
</tr>
<tr>
<td>Privacy Algorithm</td>
<td>Specifies the type of SNMPv3 cryptography privacy algorithm used.</td>
</tr>
<tr>
<td></td>
<td>• CFB-AES128</td>
</tr>
<tr>
<td></td>
<td>• CBC-DES</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Specifies the SNMPv3 privacy (encryption) password. The maximum length is 48 characters.</td>
</tr>
<tr>
<td>Notification Receiver 1</td>
<td>Enter the following information: Server Address SNMP Version Listening Port Trap/Inform</td>
</tr>
<tr>
<td>Notification Receiver 2</td>
<td>Enter the following information: Server Address SNMP Version Listening Port Trap/Inform</td>
</tr>
</tbody>
</table>
Admin Config Provisioning Profiles

Admin Config provisioning profiles, allow you to create provisioning profiles that include maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on.

You can use Admin Config provisioning profiles to provision the following Polycom endpoints:

- Polycom VVX systems deployed in dynamic management mode
- Polycom HDX systems deployed in dynamic management mode
- Polycom RealPresence Group Series endpoints (required)
- Polycom RealPresence Immersive Studio systems (required)
- Polycom CMA Desktop clients
- RealPresence Mobile clients
- RealPresence Desktop clients

If an Admin Config 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. You cannot change the name.

Polycom CMA Desktop provisioning occurs on a session by session basis.
# Available Settings for Admin Config Provisioning Profiles

The following table shows the fields you can configure when adding a new Admin Config provisioning profile to the RealPresence Resource Manager system. 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><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specify a unique name for the profile</td>
</tr>
<tr>
<td>Provisioning Profile Type</td>
<td>Choose the profile type from the drop-down list.</td>
</tr>
<tr>
<td>Selectable Provisioning for Group Series</td>
<td>When you mark this check box, you can manually select which settings within the provisioning profile are sent to a RealPresence Group system. Only the selected settings will be provisioned to RealPresence Group systems. Within the provisioning profile, only the settings that you select are set to the RealPresence Group system. For example, if a provisioning setting is blank but still checked, the blank value is still be provisioned to the system. By default, all settings are checked. If you don’t want to provision the setting to the RealPresence Group system, you must uncheck the individual settings.</td>
</tr>
<tr>
<td><strong>System Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Language Settings</td>
<td>Specifies the language for the video endpoint system’s user interface. Possible values include: Arabic, Simplified Chinese, Traditional Chinese, English_US, English_UK, French, German, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, and Spanish. If you clear this check box, the language settings can be manually configured on the endpoint.</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>Auto-answer Point to Point Calls</td>
<td>Specifies whether endpoint answers point to point calls automatically.</td>
</tr>
<tr>
<td>Auto-answer Multipoint calls</td>
<td>Specifies whether endpoint answers multipoint calls automatically.</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. <strong>Note</strong> If this setting is disabled, applications will not be able to retrieve Call Detail Report (CDR) records.</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>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems being provisioned...</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recent Calls</td>
<td>Specifies whether to display the <strong>Recent Calls</strong> button on the home screen. The <strong>Recent Calls</strong> screen lists the site number or name, the date and time, and whether the call was incoming or outgoing.</td>
</tr>
<tr>
<td>Note</td>
<td>If the <strong>Call Detail Report</strong> option is not selected, the <strong>Recent Calls</strong> option is not available.</td>
</tr>
<tr>
<td>Screen Saver Wait Time</td>
<td>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 <strong>Off</strong> prevents the system from going to sleep. To prevent image burn-in, specify 15 minutes or less.</td>
</tr>
<tr>
<td>Directory Search Mode</td>
<td>Specifies how endpoint directory searches are initiated by the endpoint user. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>—The search is executed after the user stops entering characters.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong>—The search is executed only when the user explicitly clicks the <strong>Search</strong> button.</td>
</tr>
<tr>
<td>Maximum Number of Active Web Sessions</td>
<td>Specifies the number of active web sessions that are allowed. The default is 25.</td>
</tr>
<tr>
<td>Secondary Network</td>
<td>(Pano Only) Choose a secondary network for guests to access Pano devices.</td>
</tr>
<tr>
<td>Allow Web Access on Secondary Network</td>
<td>(Pano Only) Allow administrators to access the Pano system web interface over the secondary network.</td>
</tr>
<tr>
<td><strong>Home Screen Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Display H.323 Extension</td>
<td>Lets users placing a gateway call enter the H.323 extension separately from the gateway ID.</td>
</tr>
<tr>
<td></td>
<td>If you do not select this setting, endpoint system users make gateway calls by entering the call information in this format: <code>gateway ID + ## + extension</code></td>
</tr>
<tr>
<td>Enable Availability Control</td>
<td>When enabled, lets users set their availability in the endpoint system's local user interface.</td>
</tr>
<tr>
<td>Address Bar (Left Element)</td>
<td>Allows you to select which element you want displayed on the left side of the address bar on the local interface.</td>
</tr>
<tr>
<td>Address Bar (Right Element)</td>
<td>Allows you to select which element you want displayed on the right side of the address bar on the local interface.</td>
</tr>
<tr>
<td><strong>Call Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum Speed for Receiving Calls (kbps)</td>
<td>Restricts 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.</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems being provisioned...</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Preferred Speed for Placing Calls (kbps)  | Determines the speeds that will be used for calls from this endpoint system when:  
• The Call Quality selection is either unavailable or set to Auto on the Place a Call screen  
• 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.  
The default is 384 kbps.                                                                                                                                                                                                                     |
| 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.                                                                                                                                                                                                                          |
| Enable Automatic Call Escalation          | Enable or disable the automatic call escalation feature.                                                                                                                                                                                                                                                                                                                    |
| Conference Factory ID                    | The conference factory ID created for the SIP conference factories in the RealPresence DMA System.                                                                                                                                                                                                                                                                     |
| **Audio Settings**                        |                                                                                                                                                                                                                                                                                                                                                                           |
| Mute Auto Answer Calls                    | Specifies whether or not to automatically mute incoming calls.  
The default setting is to not automatically mute incoming calls.                                                                                                                                                                                                                                                                                              |
| **CMA Desktop Settings**                  |                                                                                                                                                                                                                                                                                                                                                                           |
| Allow IM/Chat                              | When enabled, specifies that the Polycom CMA Desktop client can initiate instant messaging.  
This is enabled by default.                                                                                                                                                                                                                                                                                                                                         |
| **Software Endpoint Settings**            |                                                                                                                                                                                                                                                                                                                                                                           |
| Enable IM/Chat                             | For RealPresence Desktop clients, this option must be provisioned to support both presence and chat functions.  
For CMA Desktop, this option must be provisioned to support chat functions.                                                                                                                                                                                                                                                                                     |
| Enable Screen Saver When in Call          | Specifies whether or not to enable screen saver during a call.                                                                                                                                                                                                                                                                                                             |
| Auto Accept Invitation                    | Enables the client to auto-accept chat invitations.  
Applicable to RealPresence Desktop clients only.                                                                                                                                                                                                                                                                                                                         |
| Allow IM Storage                           | Enables the client to store chat history on its local drive.  
Applicable to RealPresence Desktop clients only.                                                                                                                                                                                                                                                                                                                         |
<p>| <strong>Note</strong>                                  | If you disable this option after enabling it, all chat history is cleared for the client.                                                                                                                                                                                                                                                                                   |</p>
<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>For the endpoint systems being provisioned...</strong></th>
</tr>
</thead>
</table>
| Provision Check that the CMA Desktop is the default program for: | • Opening Call To links  
• Opening H323 links  
• Opening SIP links  
Selecting this setting provisions the CMA Desktop to be the default program for opening the above links. |
| Provision Enable Sending 720p (HD) Video       | Select 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) is also selected.  
You can choose 15 Frames per second or 30 Frames per second.                                              |

**Calendaring Settings**

<table>
<thead>
<tr>
<th><strong>Enable Calendaring</strong></th>
<th>When enabled, this provisions the Microsoft Exchange server and calendaring settings for the endpoint system.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alert Tone</strong></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><strong>Display Private Meeting</strong></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><strong>Meeting Reminder Time</strong></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><strong>Check for New Messages Interval</strong></td>
<td>Specifies the interval to check calendar invitation messages.</td>
</tr>
</tbody>
</table>
| **Use Endpoint Provisioning Credentials** | If checked, the endpoint provisioning credentials will be used to connect the calendar server.  
If canceled, you need to go to the endpoint UI to specify the credential used to connect the calendar server. |

**Microsoft Lync Settings**

| **Group Name** | Specifies the group name for which the endpoint system should be provisioned. |

**VVX/CX Settings**

| **Configuration Server URL** | Specifies the IP address for the system that will provide provisioning service.  
All addresses can be followed by an optional directory and optional filename. |
| **Logging Server URL** | Specifies the directory to use for log files, if required.  
A URL can also be specified. This field is blank by default. |
| **Configuration Data** | Enter XML data for a custom configuration. Enables the RealPresence Resource Manager system administrator's to provision settings that the RealPresence Resource Manager system does not normally provide. |
Creating Dynamic Provisioning Rules

You apply dynamic provisioning profiles by using provisioning rules. A provisioning rule consists of one or more conditions that must be met before the dynamic provisioning profile can be applied. You can create multiple rules and associate a profile with more than one rule at a time.

For example, you can use provisioning rules to provision different endpoints within the same site with different network settings.

If a dynamically managed endpoint does not meet any conditions of any rule, it is provisioned with the default profiles.

Prioritizing Provisioning Rules

After you have added more than one provisioning rule, you can change the priority of the list of provisioning rules you created. When you add rules, they are automatically prioritized according to the order in which they were added to the system.

Rules with a higher priority will be applied first. The Rule Priority determines the order that the rules get applied.

Consider the following example:

Create two rules, one for the Support user group and one for the Toronto user group. Jason Smith is part of the Support group and also part of the Toronto group.

- The Support Rule is assigned an Admin Config provisioning profile named Low-Bandwidth, which enables a maximum speed for receiving calls of 128kbps. The Support Rule is assigned a priority of 1.
- The Toronto Rule is assigned an Admin Config provisioning profile called High-Bandwidth, which enables a maximum speed for receiving calls of 1920kbps. The Toronto Rule is assigned a priority of 2.

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

When you add provisioning rules, you may want to assign provisioning rules with more robust privileges a higher priority than those providing fewer privileges.

Using Rule Conditions

A provisioning rule is comprised of one or more conditions that you define. You are allowed to add multiple conditions of multiple condition types to a single rule.

For example, you can create a rule that applies a provisioning profile according to the user group (condition) and device type (condition).

Rule conditions can be complex and include OR or AND relationships, as well as NOT relationship.
Creating Dynamic Provisioning Rules

If a dynamically managed endpoint does not meet any conditions of any rule, it is provisioned with the default profiles.

For example, you can create a rule that applies a network provisioning profile for all device types within a site except for VVX endpoints.

Provisioning rules support the following condition types:

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>The site name.</td>
</tr>
<tr>
<td>User Group</td>
<td>The name of a user group.</td>
</tr>
<tr>
<td>User</td>
<td>You can choose from one of the following user attributes when defining a user condition for a rule:</td>
</tr>
<tr>
<td></td>
<td>• Title</td>
</tr>
<tr>
<td></td>
<td>• Department</td>
</tr>
<tr>
<td></td>
<td>• User ID</td>
</tr>
<tr>
<td>Device</td>
<td>You can choose from the following attributes when defining a device condition for a rule:</td>
</tr>
<tr>
<td></td>
<td>• Device Type</td>
</tr>
<tr>
<td></td>
<td>• Serial Number</td>
</tr>
</tbody>
</table>

**Condition Operators**

When you build conditions you can use three operators: CONTAINS, IN, and =.

The IN operator allows you to add multiple values to the same condition. For example, if you want to create a provisioning rule that applies to both RealPresence Desktop devices and RealPresence Mobile devices, you should use the IN operator and add both devices to the condition.

The IN operator is equivalent to OR but the IN performance is much better than the OR when building the rule. It is highly recommended to use IN if you want to use >= 5 ORs to connect conditions

The = operator allows you to add only one value to the condition.

The CONTAINS operator is available for user group rules.

**Working with Provisioning Rules**

When you create a provisioning rule, you can associate multiple profile types with the same provisioning rule. For example, when you provision a RealPresence Access Director for your environment, it is typical to associate a Network provisioning profile, an Admin Config provisioning profile, and a RealPresence Access Director server provisioning profile with the same rule.

If a dynamically managed endpoint does not meet any conditions of any rule, it is provisioned with the default profiles.
Add a Provisioning Rule

When you add a new provisioning rule or change its priority, 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 a work day and then let the provisioning occur at the designated polling interval.

Only users with the administrator role can add provisioning rules.

Add new provisioning rules in the middle of the work day, not first thing in the morning.

When you add a provisioning rule, use the Add New Rule dialog box to complete the following steps:

1. Create Provisioning Rule.
2. Add a Condition.
3. Associate Provisioning Profiles with a Provisioning Rule.

The following steps incorporate an example of creating a rule that applies provisioning profile to all devices of a certain type within a specific site. You can create rules of varying complexity or simplicity.

Create Provisioning Rule

Each provisioning rule you create must have a unique name as well as a description.

To create and name a provisioning rule:

2. Click Add .
   The Add New Rule dialog box displays.
3. In the General Info area, enter a name for the new rule.
   In this example, we are creating a rule for all HDX systems in the Austin, TX, area.
4 Activate or deactivate the rule.
By default, a rule is marked as active when you create it. Active rules are automatically sent the next time a dynamically managed device polls the RealPresence Resource Manager system for provisioning updates.
If you do not want the rule to be active, uncheck the Active check box.

Add a Condition
You can add a condition to a provisioning rule when you first create it or you can add a new condition or change a condition of an inactive rule.

To add a condition to a provisioning rule:

1 In the Add New Rule dialog box, click Add on the top.

The Add New Condition dialog box displays.

2 Use the Add New Condition dialog to create the conditions that you need.
   a Select a condition. In this example, we are creating a condition for the Austin site, so we chose Site in the Type drop down list, and selected the Austin site for the Value.
   b Click OK to save the condition.
       This example defines a condition for the rule to include all HDX systems.
   c To add another condition, first select the condition you just created and then click Add . To add a new condition to a rule, you must select a condition in the list from which to build on. When creating conditions, you can use the following condition operators: contains, in, or =. The contains operator is only applicable to group condition type.
       After you create the Site condition, click Add to add more conditions to your rule.
   d Select a value from the Relation column. You can relate multiple conditions with an And statement or an Or statement.
       In our example, we want this rule to apply to both the site and the device type, so we chose And. This screenshot shows a Device condition type that defines a condition that includes all HDX device types.
Creating Dynamic Provisioning Rules

After you have created your condition(s), you need to select which provisioning profiles to associate with this rule. You must have already created the provisioning profiles you need.

A provisioning rule must have at least one profile associated with the rule.

To associate provisioning profiles with a provisioning rule:

1. Click the Endpoint Provisioning Profile page in the Add New Rule dialog box.
   You can associate one or more profile to the rule. For example, one Network Provisioning Profile, one Admin Config Profile, and one Server Provisioning profile.

2. Select the Available Profiles you want to associate with the rule you created and click the down arrow to move them to the Selected Profiles section.
   In this example, you can select the HDX system profile, which is an Admin Config provisioning profile.

3. You have now finished creating a provisioning rule. Click OK to save the rule.
   These steps used an example rule that applied the associated profile to all HDX systems within a example Austin site.

Related Topics
Using Dynamic Provisioning Profiles

View Details of a Provisioning Rule
You can view the details of a provisioning rule. Use this option when you want to view the provisioning rule without editing it.
To view details of a provisioning rule:

2. Optionally, click Filter to filter the rules that display. Choose from the following filters: Rule Name, Status, and Condition (Device Type, Site, User Group).
3. In the Provisioning Rules page, select the rule you want to view.
4. Click View Details.
5. Click OK.

Edit the Priority of a Provisioning Rule

By default, provisioning rules are assigned a priority level according to order in which they are added to the system. You can change the priority of a provisioning rule.

Provisioning rules with higher priority get applied first.

To edit the priority of a provisioning rule:

2. Optionally, click Filter to filter the rules that display. Choose from the following filters: Rule Name, Status, and Condition (Device Type, Site, User Group).
3. In the Provisioning Rules page, select the rule of which you want to change the priority.
4. Click Edit Priority from the More drop-down list.
   The Edit Priority dialog appears.
5. Enter a new priority number in the Rule Priority field.
6. Click OK.
   The system changes the priority of the selected provisioning rule.

Clone a Provisioning Rule

You can clone a provisioning rule when you want to re-use most of its conditions in a new rule or just change the name of an existing rule.

To clone a provisioning rule:

2. Optionally, click Filter to filter the rules that display. Choose from the following filters: Rule Name, Status, and Condition (Device Type, Site, User Group).
3. In the Provisioning Rules page, select the rule you want to clone and click Clone.
4. In the Clone Rule dialog box, enter a name for the new rule and click Save.
   The provisioning rule appears last in the Provisioning Rules list.
5. As needed, edit the rule.
Deactivate a Provisioning Rule

You can deactivate a provisioning rule if you want to stop using it as a provisioning rule or edit it. Deactivated provisioning rules are not used.

You must activate a provisioning rule for it to be used.

To deactivate a provisioning rule:

2. Optionally, click Filter ➤ to filter the rules that display. Choose from the following filters: Rule Name, Status, and Condition (Device Type, Site, User Group).
3. In the Provisioning Rule page, select the rule and select More > Deactivate.
4. Click Yes to confirm the deactivation.

Edit a Provisioning Rule

When you choose to edit a provisioning rule, it automatically becomes deactivated. If you want to view the details of a provisioning rule without de-activating it, use the View Details option.

If you choose not to save your changes, the rule will not be deactivated.

To edit a provisioning rule:

2. Optionally, click Filter ➤ to filter the rules that display. Choose from the following filters: Rule Name, Status, and Condition (Device Type, Site, User Group).
3. Select the rule and click Edit ↗.
   You are prompted to deactivate the rule.
4. Click OK to confirm the deactivation.
5. In the Edit Rule dialog box, make your changes.
6. Click OK.
   The provisioning rule is updated.

Delete a Provisioning Rule

You cannot delete an active provisioning rule. You must first deactivate it before you can delete it.

To delete an provisioning rule:

2. Optionally, click Filter ➤ to filter the rules that display. Choose from the following filters: Rule Name, Status, and Condition (Device Type, Site, User Group).
3. Select the rule and click Delete ✗.
Stop Dynamic Management of an Endpoint

If you want to stop dynamically managing an endpoint, you must first disable the provisioning service settings on the endpoint.

To stop dynamic management for a Polycom HDX system, see the Polycom HDX documentation.

To stop dynamically managing an endpoint:

1. From the endpoint’s web interface, navigate to the Provisioning Service settings and cancel the **Enable Provisioning** check box.
2. From the RealPresence Resource Manager system, navigate to **Endpoint > Monitor View**, highlight the endpoint and click **Delete** ❌.
Dynamically Managing Endpoint Naming Schemes

The RealPresence Resource Manager system allows administrators to configure their E.164 alias, endpoint naming schemes and SIP URIs for endpoints that are dynamically managed.

If you choose to provision H.323 settings through a network provisioning profile, you can also define the E.164 number and endpoint naming scheme used for endpoints. You can also auto-generate SIP URIs for dynamically managed endpoints.

Using Custom Active Directory Attributes

When your system is integrated with Active Directory, it only incorporates and displays attributes from the Active Directory record that are part of the Active Directory Global Catalog. When you define E.164 numbers and SIP URIs, you can use Active Directory attributes that are not displayed in the RealPresence Resource Manager system user record.

For example, the following diagram displays some telephone numbers that can be configured in Active Directory. By default, when you integrate your RealPresence Resource Manager system with Active Directory only the default phone number field is used within the E.164 Numbering scheme.

If you wanted use the IP Phone attribute instead of the default phone number, you need to enter that specific attribute name that in RealPresence Resource Manager system when you create a naming scheme.

The following screen shot displays the IP Phone attribute being entered when you create an E.164 naming scheme:
**Find the Attribute Name to Use**

You must use the correct name of the attribute. You can use the Active Directory management console to find the attribute name you want to use.

To use Active Directory to find an attribute name:

1. Select **View > Advanced Features** to ensure advanced features are enabled in the console.
2. Navigate to an Active Directory user.
3. Right-click the user and select **Properties**.
4. In the **Properties** dialog, click the **Attribute Editor** tab.
5. Find the attribute to be used and record the attribute name.

6. Use the **Attribute** name as the value in **Mapping to Active Directory Name** field.

**Active Directory Global Service**

The Active Directory global catalog is a distributed data repository that contains a search-able, partial representation of every object in every domain in a multi-domain Active Directory Domain Services (Active Directory DS) forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multi-master replication. Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.
However, to minimize replication traffic and keep the global catalog's database small, only selected attributes of each object are replicated. This is called the partial attribute set (PAS). The PAS can be modified by modifying the schema and marking attributes for replication to the global catalog.

The Active Directory administrator can do this by ensuring that the corresponding attributes are included in the Partial Attribute Set. See http://support.microsoft.com/kb/248717 for information about “How to Modify Attributes That Replicate to the Global Catalog.”

To take advantage of custom Active Directory attributes in RealPresence Resource Manager, your Active Directory administrator must ensure that the attributes you want to use have been added to the Active Directory Global Catalog service.

You must work with your Active Directory administrator to decide how to manipulate the Active Directory schema to ensure that the attributes you want to use in naming schemes are available to the RealPresence Resource Manager system.

**Define an E.164 Address Scheme**

You can define an E.164 address scheme that will be used when provisioning E.164 addresses to all dynamically managed endpoints.

You can choose to use to define a number range, use the default phone number or use a different Active Directory attributes.

**To define an E.164 address scheme for dynamically managed endpoints:**

1. Navigate to **Endpoint > Dynamic Management > E.164 Numbering**.
2. Define your numbering scheme according to the options provided.

   The total number of digits specified for an E.164 number must be 15 or less. If the user's phone number is used as the base field, the system reserves one digit to differentiate between the user's multiple devices. In this case the total number of digits configured cannot exceed 14 digits.

3. When finished defining your numbering scheme, click **Update**.

   The settings only can be applied to new added dynamically managed endpoints but existing endpoints will not be impacted.

   See **Managing Dial String Reservations for Users** on how to update the name or number on existing endpoints.

**E.164 Numbering Scheme Settings**

The administrator has the following options when implementing an E.164 numbering scheme:
Specify Base Field

You can define a specific number range or indicate that a phone number be used for the **Base Field**.

**To specify the Base Field:**

1. In the **Base Field**, select one of the followings:
   - **Specify Number Range.**
     - Use the **To** and **From** fields to define the number range.
   - **Use Phone Number**
     - If you want to use the main phone number field from Active Directory, leave the **Mapping to Active Directory Name** field blank.
     - If you want to use a number other than the one indicated in the **Phone Number** field in **Active Directory**, you can indicate another Active Directory attribute to use.
     - For example, if your Active Directory also includes mobile number information in an Active Directory Attribute called `mobilenum`, you should select **Use Phone Number** and then enter the name `mobilenum` in the **Mapping to Active Directory Name** field.
     - Enter the **Maximum number of digits to use** from the user’s phone number (between 3 and 10 digits). The digits from the phone number are selected from right to left.
c Enter Number range to use if phone number is empty (reverts to Specify Number Range) — The system will revert to using a number range if the user’s phone number is empty.

### Define an Endpoint Naming Scheme and H.323 Alias

You can define an endpoint naming scheme that will be provisioned to all dynamically managed endpoints. When you define the endpoint name, you can choose to have the endpoint name also serve as the H.323 alias for the endpoint. This is the default.

Alternatively, you can use a different name for the H.323 alias and the endpoint name and define a naming scheme for both.

System names cannot exceed 36 characters or provisioning will fail.

### To define an endpoint naming scheme for dynamically managed endpoints:

1. Navigate to **Endpoint > Dynamic Management > Endpoint Naming**.
2. Build your endpoint naming scheme.
   - System names can be a combination of up to four naming fields and three separators. For example, the following endpoint name is defined by selecting UserID, City and Endpoint Type fields and by using two "." separators: UserID.City.HDX.
3. To use the endpoint name as the hostname for hardware endpoints (such as RealPresence Group Series, HDX, or RealPresence Immersive Studio systems), select the **Use the Generated Endpoint Name as the Hardware Endpoint’s Hostname** check box.
4. To use same naming scheme for the H.323 alias, ensure that the **Use Endpoint Naming for H323 ID** check box is selected.
5. To use a different naming scheme for the H.323 alias:
   a. Clear the **Use Endpoint Naming for H323 ID** check box.
   b. Build your H.323 ID scheme according to the same options as the System Name.
6. When finished, click **Update**.
   - The settings only can be applied to new added dynamically managed endpoints but existing endpoints will not be impacted.
   - See **Managing Dial String Reservations for Users** on how to update number on existing endpoints.
   - See **Edit an Endpoint** on how to update endpoint system name.

### Related Topics

- Endpoint Naming Scheme
- H.323 ID Scheme
**Endpoint Naming Scheme**

The administrator has the following options when implementing an endpoint naming scheme:

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Area</td>
<td>When areas are enabled, you can select an area to which you want to apply this endpoint naming scheme. This field is only available to users who manage more than one area. The drop-down list lists only those areas that the user has permission to manage.</td>
</tr>
</tbody>
</table>
| Naming Field    | The following fields are available to use as a naming field. Be sure that the field you choose is populated for all users in your system. You cannot use the same naming field twice in the same scheme.  
• Last Name  
• First Name  
• User ID  
• City  
• Department  
• Endpoint Type  
• Domain  
• Title  
• Area (only available when areas are enabled)  
You cannot use the same naming field more than once within the same naming scheme. |
| Separator       | You can use a separator between each naming field. If you do not want to use a separator, you must select (none).  
Choose from the following separators:  
• (none)  
• (space)  
• ,  
• –  
• _  
You can use the same separator multiple times. |

**H.323 ID Scheme**

The administrator has the following options for an H.323 ID scheme:
<table>
<thead>
<tr>
<th>Option</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Area</td>
<td>When areas are enabled, you can select an area to which you want to apply this endpoint naming scheme. This field is only available to users who manage more than one area. The drop-down list lists only those areas that the user has permission to manage.</td>
</tr>
<tr>
<td>Naming Field</td>
<td>The following fields are available to use as a naming field. Be sure that the field you choose is populated for all users in your system. You cannot use the same naming field twice in the same scheme.</td>
</tr>
<tr>
<td></td>
<td>• Last Name</td>
</tr>
<tr>
<td></td>
<td>• First Name</td>
</tr>
<tr>
<td></td>
<td>• User ID</td>
</tr>
<tr>
<td></td>
<td>• City</td>
</tr>
<tr>
<td></td>
<td>• Department</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Type</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Model</td>
</tr>
<tr>
<td></td>
<td>• Domain</td>
</tr>
<tr>
<td></td>
<td>• Title</td>
</tr>
<tr>
<td></td>
<td>• Area (only available when areas are enabled)</td>
</tr>
<tr>
<td></td>
<td>You cannot use the same naming field more than once within the same naming scheme.</td>
</tr>
<tr>
<td>Separator</td>
<td>You can use a separator between each naming field. If you do not want to use a separator, you must select (none).</td>
</tr>
<tr>
<td></td>
<td>Choose from the following separators:</td>
</tr>
<tr>
<td></td>
<td>• (none)</td>
</tr>
<tr>
<td></td>
<td>• -</td>
</tr>
<tr>
<td></td>
<td>• _</td>
</tr>
<tr>
<td></td>
<td>You can use the same separator multiple times.</td>
</tr>
</tbody>
</table>
Auto-Generate SIP URIs for Dynamically Managed Endpoints

You can automatically generate a SIP URI for each dynamically managed endpoint according to a naming scheme you define.

You can choose to use the user e-mail address as the SIP URI or define a custom URI from Active Directory attributes.

When you define a custom SIP URI from Active Directory fields, you can choose one of the default fields or an different Active Directory attribute.

To auto-generate SIP URIs for dynamically managed endpoints:

1. Navigate to Endpoint > Dynamic Management > SIP URI.
2. If areas are enabled, select an area from the Select Area drop-down list.
   - The Select Area drop-down list is available to users with the administrator or area administrator role. The areas included in the list are restricted to those areas that the user is allowed to manage.
3. Select the Auto-generate SIP URIs for all users check box.
   - You can either use the user’s e-mail address as the SIP URI or define the SIP URI yourself.
4. To use the user’s e-mail address as their SIP URI. Check the Use the user’s e-mail address as their SIP URI if you want this option.
   - If you choose this option, you cannot further define the fields used for the SIP URI.
5. To define a SIP URI, complete the naming fields and separators.
   - SIP URIs can be a combination of up to four naming fields, three separators and domain name suffix. For example, the following SIP URI is defined by selecting UserID, City and Endpoint Type fields, by using two "." separators and domain name "abc.com": UserID.City.HDX@abc.com.
   - You can use a pre-defined naming field from the drop-down list or type a specific Active Directory attribute.
     a. To use a pre-defined field, select it from the drop-down list. Pre-defined fields include: Last Name, First Name, User ID, City, Department, Endpoint Type, Endpoint Model, Domain, and Title.
     b. To use an Active Directory attribute, select AD Attribute from the drop-down list and enter the name of the attribute in the Attribute Name field. The attribute you enter must exactly match an existing Active Directory attribute. Talk to your Active Directory administrator if you have questions about which Active Directory attributes are available for use.
   - As a best practice, include be sure to include a valid SIP Domain information in the SIP URI definition.
6. Select the Keep URIs Unique check box if you want unique SIP URIs for each endpoint regardless of user.
   - If you leave this check box cleared, the user’s SIP URI can be used for each endpoint associated with that user.
7 Click **Update**.

The settings only can be applied to new added dynamically managed endpoints but existing endpoints will not be impacted.

See [Managing Dial String Reservations for Users](#) on how to update the name or number on existing endpoints.

**SIP Domain Information**

The table explains the SIP domain information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naming Field</td>
<td>The following fields are available to use as a naming field. Be sure that the field you choose is populated for all users in your system. You cannot use the same naming field twice in the same scheme.</td>
</tr>
<tr>
<td></td>
<td>• Last Name</td>
</tr>
<tr>
<td></td>
<td>• First Name</td>
</tr>
<tr>
<td></td>
<td>• User ID</td>
</tr>
<tr>
<td></td>
<td>• City</td>
</tr>
<tr>
<td></td>
<td>• Department</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Type</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Model</td>
</tr>
<tr>
<td></td>
<td>• Domain</td>
</tr>
<tr>
<td></td>
<td>• Title</td>
</tr>
<tr>
<td></td>
<td>• AD Attribute.</td>
</tr>
<tr>
<td></td>
<td>▲ When you select AD attribute, you must also enter an name in the <strong>Attribute Name</strong> field. The name must match an available Active Directory attribute. You cannot use the same naming field more than once within the same naming scheme.</td>
</tr>
</tbody>
</table>
## Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage</th>
</tr>
</thead>
</table>
| Separator           | You can use a separator between each naming field. If you do not want to use a separator, you must select (none). Choose from the following separators:  
• (none)  
• .  
• _  
• @  
You cannot use the @ separator more than once and it cannot be used before the _ separator. |
| Domain name suffix  | Adds the domain suffix to the naming field you choose.  
You can either choose None or select “A String (specify) to enter the domain suffix as a string value.  
For example, LastName.FirstName@domainsuffix.com can be defined by selecting LastName and FirstName as naming fields with a “.” separator. The Domain suffix in this example was entered as a string.  
**Caution:** Be sure to verify that the string you enter here is a valid SIP domain or the SIP URI will not be valid. |
Using Bundled Provisioning Profiles

The Polycom RealPresence Resource Manager system supports Bundled Provisioning Profiles for dynamically managed Polycom RealPresence Group Series systems, Polycom RealPresence Immersive Studio systems, RealPresence Centro, and Polycom HDX (v3.0.3 and higher) systems. With Bundled Provisioning Profiles, a RealPresence Resource Manager user with the administrator role can download a bundled provisioning profile from any already configured endpoint that is dynamically managed by the RealPresence Resource Manager.

You can then indicate which supported dynamically managed endpoint of the same model and software version will receive the bundled provisioning profile when it next polls the RealPresence Resource Manager system for new provisioning information.

Bundled provisioning profiles are one of three types of provisioning profiles that you can use when dynamically managing an endpoint.

Bundled provisioning profiles provides businesses with an efficient and effective way to provision RealPresence Group Series, RealPresence Immersive Studio systems, and Polycom HDX systems consistently across each model. Endpoint users with administrative rights can still change the settings on an HDX system after the bundled provisioning profile is applied. However, if another profile is sent by the RealPresence Resource Manager system, it will overwrite the user’s changes.

How Bundled Provisioning Works

In dynamic management mode, when a Polycom endpoint starts up and at designated intervals thereafter, it automatically polls for new provisioning information from the RealPresence Resource Manager system. If a bundled provisioning profile exists on the RealPresence Resource Manager system that has been associated with the endpoint, the bundled profile is sent over a secure HTTPS connection.

In this release, the RealPresence Group Series, RealPresence Immersive Studio systems, and HDX system (v3.0.3 and higher) parameters that may be included in a bundled provisioned profile are limited to the following types:

- Camera configuration settings
- Monitor configuration settings
- Microphone configuration settings
- Security settings (such as password length)
- Home screen settings
Using Bundled Provisioning Profiles

Considerations for Bundled Provisioning Profiles

Consider the following items when using bundled provisioning profiles.

- You can store a maximum of 1000 bundled provisioning profiles on your RealPresence Resource Manager system.
- You cannot update software with a bundled profile.
- The software version of the endpoint must match the software version of the endpoint from which the bundled provisioning profile was made. A bundled profile is only compatible with endpoints of the same software version. If the endpoint’s software version is updated, you must create a new bundled profile.
- When using bundled provisioning profiles to provision HDX systems, you can use them with v3.0.3 or higher. Previous versions do not support bundled provisioning profiles.
- Security and home screen settings are not included in bundled profiles for RealPresence Group Series.
- You must have the Administrator role to create bundled provisioning profiles. Users with the Device Administrator role can apply and re-assign bundled provisioning profiles.
- Be sure to give each provisioning profile a unique name.

Download a Bundled Provisioning Profile

You can download a bundled provisioning profile from any RealPresence Group Series, RealPresence Immersive Studio system, or HDX system that is registered with the RealPresence Resource Manager system. After you download a provisioning profile for a specific endpoint, all dynamically-managed HDX endpoints that you associate with this profile will receive the provisioning profile when the HDX system next polls the RealPresence Resource Manager system for new provisioning information.

To download a bundled provisioning profile:

1. Go to Endpoint > Dynamic Management > Bundled Provisioning Profiles.
2. Click Download.
   - The Download Bundled Provisioning Profile From an Endpoint dialog lists all of the HDX systems and Group Series registered with the system, up to 500 endpoints.
3. As needed, click Filter to customize the endpoint list.
4. Select the endpoint that is configured the way you want for the bundled provisioning profile.
5. Complete the Bundled Provisioning Profile Name and Description fields.
6. Click Download.
   - The system confirms that the profile downloaded successfully.
7. Click OK.

View the List of Bundled Provisioning Profiles

Use the Bundled Provisioning View to see the list of bundled provisioning profiles available to dynamically managed RealPresence Group Series, RealPresence Immersive Studio systems and HDX systems.
To view a list of bundled provisioning profiles:

1. Go to Endpoint > Dynamic Management > Bundled Provisioning Profiles.
   
   By default the Bundled Provisioning Profile View displays the list of bundled provisioning profiles available for use by dynamically managed HDX systems and RealPresence Group Series.

2. As needed, click Filter to customize the endpoint list. The filter provides the following options:
   - **Profile Name** Filters by the name of the bundled provisioning profile.
   - **Model** Filters by the endpoint model.
   - **Software Version** Filters by the software version of the endpoint.
   - **Creation Date** Filters by the date the bundled provisioning profile was downloaded and created on the system.
   - **Description** Filters by the description of the bundled provisioning profile.

   The profile list in the Bundled Provisioning Profile View has the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>The name assigned to the bundled provisioning profile when it was downloaded and created on the system.</td>
</tr>
<tr>
<td>Model</td>
<td>The exact model of endpoint to which the bundled provisioning profile applies as defined when it was downloaded and created on the system.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Displays the software version of the endpoint from which the bundled provisioning profile was downloaded.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>The date the bundled provisioning profile was downloaded and created on the system.</td>
</tr>
<tr>
<td>Description</td>
<td>The description assigned to the bundled provisioning profile when it was downloaded and created on the system.</td>
</tr>
<tr>
<td>Device Count</td>
<td>The number of devices that are associated with the bundled provisioning profile.</td>
</tr>
</tbody>
</table>

### Edit a Bundled Provisioning Profile

Users with the administrator role are allowed to edit bundled provisioning profiles. When you edit a bundled provisioning profile you can rename the profile or change which devices are associated with the profile.

To edit a bundled provisioning profile:

1. Go to Endpoint > Dynamic Management > Bundled Provisioning Profiles.

2. As needed, click Filter to customize the list of profiles.

3. Select the profile that you want to edit.

4. Click **Edit** to view the Edit Bundled Provisioning Profile dialog box.

5. Use the Edit Bundled Provisioning Profile dialog to edit the profile and click **OK**.
Delete a Bundled Provisioning Profile

When you no longer need a bundled provisioning profile, you can delete it.

1. Go to Endpoint > Dynamic Management > Bundled Provisioning Profiles.
2. As needed, click Filter 🔄 to customize the list of bundled provisioning profiles.
3. Select the profile you want to delete.
4. Click Delete ✗.
5. Click Yes to confirm the deletion.

The system confirms that the profile was deleted.

Re-associate Devices with a Different Profile

Users with the administrator role can re-associate devices with a different bundled provisioning profile or no bundled profile. For example, you could use this feature if you previously associated all RealPresence Group 300 systems with a specific profile, but then downloaded an updated bundled provisioning profile that you would like to use instead.

To re-associate devices with a different bundled provisioning profile:

1. Go to Endpoint > Dynamic Management > Bundled Provisioning Profiles.
2. Select the profile from which you want to remove the associated devices.
3. Click **More > Re-associate Devices** to view the **Move Associated Devices** dialog.
4. Choose a profile (or None) from the list to move the associated devices.
5. Click **OK**.

**Settings included in a Bundled Provisioning Profile for an HDX**

The following tables lists the settings contained in a bundled provisioning profile for an HDX system.

<table>
<thead>
<tr>
<th>Field</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home Screen Settings</strong></td>
<td>System Name (Display)</td>
</tr>
<tr>
<td></td>
<td>Local Date and Time (Display)</td>
</tr>
<tr>
<td></td>
<td>System (Display)</td>
</tr>
<tr>
<td></td>
<td>Availability Control (Display)</td>
</tr>
<tr>
<td></td>
<td>My SIP (Display)</td>
</tr>
<tr>
<td></td>
<td>My IP (Display)</td>
</tr>
<tr>
<td></td>
<td>My ISDN (Display)</td>
</tr>
<tr>
<td></td>
<td>My Extension (Display)</td>
</tr>
<tr>
<td></td>
<td>Home Button (1-6)</td>
</tr>
<tr>
<td></td>
<td>Speed Dial (all)</td>
</tr>
<tr>
<td><strong>Place a call</strong></td>
<td>Last Number Displayed</td>
</tr>
<tr>
<td></td>
<td>Call Quality</td>
</tr>
<tr>
<td><strong>Password Settings</strong></td>
<td>Minimum Length</td>
</tr>
<tr>
<td>Admin Room</td>
<td>Require Lower Case</td>
</tr>
<tr>
<td></td>
<td>Require Upper Case</td>
</tr>
<tr>
<td></td>
<td>Require Numbers</td>
</tr>
<tr>
<td></td>
<td>Require Special Characters</td>
</tr>
<tr>
<td></td>
<td>Reject Previous Passwords</td>
</tr>
<tr>
<td></td>
<td>Minimum Password Age in Days</td>
</tr>
<tr>
<td></td>
<td>Maximum Password Age in Days</td>
</tr>
<tr>
<td></td>
<td>Password Expiration Warning in Days</td>
</tr>
<tr>
<td></td>
<td>Minimum Changed Characters</td>
</tr>
<tr>
<td></td>
<td>Maximum Consecutive Repeated Characters</td>
</tr>
<tr>
<td></td>
<td>Can contain ID or its Reverse Form</td>
</tr>
<tr>
<td>Field</td>
<td>Minimum Length</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Admin Remote</td>
<td></td>
</tr>
<tr>
<td>User Room</td>
<td></td>
</tr>
<tr>
<td>User Remote</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Options</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Meeting</td>
<td>Minimum Length&lt;br&gt;Require Lower Case&lt;br&gt;Require Upper Case&lt;br&gt;Require Numbers&lt;br&gt;Require Special Characters&lt;br&gt;Reject Previous Passwords&lt;br&gt;Minimum Password Age in Days&lt;br&gt;Maximum Password Age in Days&lt;br&gt;Password Expiration Warning in Days&lt;br&gt;Minimum Changed Characters&lt;br&gt;Maximum Consecutive Repeated Characters&lt;br&gt;Can contain ID or its Reverse Form</td>
</tr>
<tr>
<td>Require Numbers: User Room</td>
<td></td>
</tr>
</tbody>
</table>

**LDAP Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LDAP Global Directory</td>
<td>Specify whether to allow endpoint systems to connect to the Polycom RealPresence Resource Manager system LDAP directory, which includes both local and enterprise users and groups. If this check box is unchecked then the provisioned endpoint will not search the Polycom RealPresence Resource Manager system LDAP directory. The endpoint system will display groups and users local to endpoint.</td>
</tr>
<tr>
<td>LDAP Default Group</td>
<td>Specify a default contact group for the endpoints systems. Set to <strong>All</strong> or to a specific local or enterprise group.</td>
</tr>
</tbody>
</table>

**Account Management**

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Account After Failed Logins: Admin</td>
<td></td>
</tr>
<tr>
<td>Lock Account Duration in Minutes: Admin</td>
<td></td>
</tr>
<tr>
<td>Lock Account After Failed Logins: User</td>
<td></td>
</tr>
<tr>
<td>Lock Account Duration in Minutes: User</td>
<td></td>
</tr>
</tbody>
</table>

**Log Management**

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percent Filled Threshold</td>
<td></td>
</tr>
<tr>
<td>Log File Name</td>
<td></td>
</tr>
<tr>
<td>Folder Name</td>
<td></td>
</tr>
<tr>
<td>Transfer Frequency</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Monitor 1</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Format</td>
</tr>
<tr>
<td></td>
<td>Resolution</td>
</tr>
<tr>
<td></td>
<td>Output Upon Screen Saver Activation</td>
</tr>
<tr>
<td></td>
<td>Display Near Video</td>
</tr>
<tr>
<td></td>
<td>Display Far Video</td>
</tr>
<tr>
<td></td>
<td>Display Content</td>
</tr>
<tr>
<td></td>
<td>Monitor 2</td>
</tr>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Format</td>
</tr>
<tr>
<td></td>
<td>Resolution</td>
</tr>
<tr>
<td></td>
<td>Output Upon Screen Saver Activation</td>
</tr>
<tr>
<td></td>
<td>Display Near Video</td>
</tr>
<tr>
<td></td>
<td>Display Far Video</td>
</tr>
<tr>
<td></td>
<td>Display Content</td>
</tr>
<tr>
<td></td>
<td>Monitor 3</td>
</tr>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Format</td>
</tr>
<tr>
<td></td>
<td>Resolution</td>
</tr>
<tr>
<td></td>
<td>Output Upon Screen Saver Activation</td>
</tr>
<tr>
<td></td>
<td>Display Near Video</td>
</tr>
<tr>
<td></td>
<td>Display Far Video</td>
</tr>
<tr>
<td></td>
<td>Display Content</td>
</tr>
<tr>
<td></td>
<td>Display Copy of Monitor 1/2</td>
</tr>
<tr>
<td></td>
<td>Monitor 4</td>
</tr>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Format</td>
</tr>
<tr>
<td></td>
<td>Resolution</td>
</tr>
<tr>
<td></td>
<td>Output Upon Screen Saver Activation</td>
</tr>
<tr>
<td></td>
<td>Loop Selected Camera to Monitor 4</td>
</tr>
<tr>
<td>People Video Adjustment</td>
<td></td>
</tr>
<tr>
<td>Content Video Adjustment</td>
<td></td>
</tr>
<tr>
<td>Dual Monitor Emulation</td>
<td></td>
</tr>
<tr>
<td>Display Icons in a Call</td>
<td></td>
</tr>
<tr>
<td>Screen Saver Wait Time</td>
<td></td>
</tr>
<tr>
<td>PIP Timer</td>
<td></td>
</tr>
<tr>
<td><strong>Multipoint Setup</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Auto Answer Multipoint Video</td>
</tr>
<tr>
<td></td>
<td>Multipoint Mode</td>
</tr>
<tr>
<td><strong>Cameras</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Camera 1</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Quality (Motion/Sharpness setting)</td>
</tr>
<tr>
<td></td>
<td>Source (People/Content setting)</td>
</tr>
<tr>
<td>Camera 2</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Quality (Motion/Sharpness setting)</td>
</tr>
<tr>
<td></td>
<td>Source (People/Content setting)</td>
</tr>
<tr>
<td>Camera 3</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Quality (Motion/Sharpness setting)</td>
</tr>
<tr>
<td></td>
<td>Source (People/Content setting)</td>
</tr>
<tr>
<td>Camera 4</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Quality (Motion/Sharpness setting)</td>
</tr>
<tr>
<td></td>
<td>Source (People/Content setting)</td>
</tr>
<tr>
<td>Camera 5</td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Aspect Ratio</td>
</tr>
<tr>
<td></td>
<td>Video Quality (Motion/Sharpness setting)</td>
</tr>
<tr>
<td></td>
<td>Source (People/Content setting)</td>
</tr>
<tr>
<td>Far Control of Near Camera</td>
<td></td>
</tr>
<tr>
<td>Backlight Compensation</td>
<td></td>
</tr>
<tr>
<td>Primary Camera</td>
<td></td>
</tr>
<tr>
<td>Camera Pan Direction</td>
<td></td>
</tr>
<tr>
<td>Quality Preference</td>
<td></td>
</tr>
<tr>
<td>Dynamic People/Content Bandwidth</td>
<td></td>
</tr>
<tr>
<td>Power Frequency</td>
<td></td>
</tr>
</tbody>
</table>

### SIP Settings

<p>| Enable SIP | Specify whether to enable SIP calls. |
| Proxy Server | Specify the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, no proxy server is used. By default, the SIP signaling is sent to port 5060 on the proxy server. To specify a different port, add it to the address as shown here: 10.11.12.13:5070 |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Protocol</td>
<td>Indicates the protocol the endpoint system uses for SIP signaling. The SIP network infrastructure determines which protocol is required.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong> enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TLS</strong> provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TCP</strong> provides reliable transport via TCP for SIP signaling.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UDP</strong> provides best-effort transport via UDP for SIP signaling.</td>
</tr>
<tr>
<td>Maximum Time in Call (minutes)</td>
<td>Enter the maximum number of minutes allowed for calls on the endpoint systems. When this time has expired, endpoint system users see a message asking</td>
</tr>
<tr>
<td></td>
<td>them if they want to hang up or stay in the call. If they do not answer within one minute, the call automatically disconnects. If they choose to stay in</td>
</tr>
<tr>
<td></td>
<td>the call at this time, they will not be prompted again. Set this value to 0 to remove any limit.</td>
</tr>
<tr>
<td>Recent Calls</td>
<td>Specify whether to display the <strong>Recent Calls</strong> button on the endpoint system’s home screen. The <strong>Recent Calls</strong> page lists the site number or name, the date and time, and whether the call was incoming or outgoing.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If the <strong>Call Detail Report</strong> option is not selected, the <strong>Recent Calls</strong> option is not available.</td>
</tr>
<tr>
<td>Screen Saver Wait Time</td>
<td>Specify how long the endpoint systems should remain awake during periods of inactivity. The default is 3 minutes. Setting this option to <strong>Off</strong> prevents</td>
</tr>
<tr>
<td></td>
<td>the system from going to sleep.</td>
</tr>
<tr>
<td>Address Displayed in Global Directory</td>
<td>Specify whether to display the endpoint systems’ public or private address in the Global Address Book.</td>
</tr>
<tr>
<td>Send Content When PC Connects</td>
<td></td>
</tr>
<tr>
<td>Camera Icon Category</td>
<td></td>
</tr>
<tr>
<td>People On Content</td>
<td><strong>Foreground Source</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Background Source</strong></td>
</tr>
</tbody>
</table>

Polycom, Inc. 345
<table>
<thead>
<tr>
<th>Field</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audio Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Sound Effects Volume | Sound Effects Volume  
Incoming Video Call Tone  
User Alert Tone  
Mute Auto Answer Calls  
Enable Live Music Mode  
Mute Auto Answer Calls  
Enable Live Music Mode  
Enable Keyboard Noise Reduction  
Enable Polycom Microphones  
Enable Hawkeye Microphones |
| **Audio Input**   |                                                                           |
| Content Input Level |                                                                           |
| Line Input Level   |                                                                           |
| Line Input Type (Line, Mic) |                                                                     |
| Line Input Canceler Enable |                                                                     |
| Enable Phantom Power (for Mic Input mode) |                                                              |
| **Audio Output**  |                                                                           |
| Line Output Mode   |                                                                           |
| Line Output Level   |                                                                           |
| VCR/DVD Output Level |                                                                     |
| VCR/DVD Output On   |                                                                           |
| Master Audio Volume |                                                                           |
| Bass   |                                                                           |
| Treble |                                                                           |
| **Stereo Settings** |                                                                           |
| Enable Polycom StereoSurround |                                                                     |
| Stereo Auto Rotation (per Mic) |                                                                     |
| Mic Mode (Left, Left+Right, Right) |                                                     |
## Settings included in a Bundled Provisioning Profile for a RealPresence Group System and RealPresence Immersive Studio System

The following tables list the settings contained in a bundled provisioning profile for a RealPresence Group system as well as RealPresence Immersive Studio systems.

<table>
<thead>
<tr>
<th>Field</th>
<th>Monitor 1</th>
<th>Monitor 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitors</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor 1</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td>Video Format</td>
<td>Video Format</td>
</tr>
<tr>
<td></td>
<td>Resolution</td>
<td>Resolution</td>
</tr>
<tr>
<td>Monitor 2</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td>Video Format</td>
<td>Video Format</td>
</tr>
<tr>
<td></td>
<td>Resolution</td>
<td>Resolution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Monitor 1</th>
<th>Monitor 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitors</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor 1</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td>Video Format</td>
<td>Video Format</td>
</tr>
<tr>
<td></td>
<td>Resolution</td>
<td>Resolution</td>
</tr>
<tr>
<td>Monitor 2</td>
<td>Enable</td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td>Video Format</td>
<td>Video Format</td>
</tr>
<tr>
<td></td>
<td>Resolution</td>
<td>Resolution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Sleep</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sleep</strong></td>
<td></td>
</tr>
<tr>
<td>Sleep</td>
<td>Display</td>
</tr>
<tr>
<td></td>
<td>Time before system goes to sleep</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Input1: Main</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Video Inputs</strong></td>
<td></td>
</tr>
<tr>
<td>General Camera</td>
<td>Allow other participants in a call to control your camera</td>
</tr>
<tr>
<td></td>
<td>Power Frequency</td>
</tr>
<tr>
<td></td>
<td>Make this camera your main camera</td>
</tr>
<tr>
<td>Settings</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Model</td>
</tr>
<tr>
<td>Display As</td>
<td>Name</td>
</tr>
<tr>
<td>Input Format</td>
<td>Display As</td>
</tr>
<tr>
<td>Optimized for</td>
<td>Input Format</td>
</tr>
<tr>
<td>White Balance</td>
<td>Optimized for</td>
</tr>
<tr>
<td>Brightness</td>
<td>White Balance</td>
</tr>
<tr>
<td>Color Saturation</td>
<td>Brightness</td>
</tr>
<tr>
<td>Field</td>
<td>Options</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Input2: Main</td>
<td>Name, Display As, Input Format, Optimized for, Backlight compensation, White Balance, Brightness, Color Saturation</td>
</tr>
</tbody>
</table>

### Audio

**General Audio Settings**
- Polycom Stereo Sound
- Sound Effects volume
- Ringtone
- User Alert Tones
- Mute Auto Answer Calls
- Enable Music Mode
- Enable Keyboard Noise Reduction
- Enable Polycom Microphones

**Audio Input**
- Use 3.5 mm Input for Microphone
- HDMI Input (left/right)
- 3.5 mm (left/right)

**Audio Output**
- Line Output Mode

**Levels**
- Master Audio Volume
- Bass
- Treble

### Security > Local Accounts

**Account Lockout**
- Lock User Account After Failed Logins

**Login Credentials**
- Admin Room Password
- User Remote Access Password
- Require User Login for System Access

**Password Requirements**
All password requirements for the following passwords:
- Admin Room
- User Room
- Meeting
- Remote Access

### General Setting > Pairing > Polycom Touch Control

**Enable Polycom Touch Control**
Using Access Control Lists

The Polycom® RealPresence® Resource Manager system enables you to create Access Control Lists for dynamically managed endpoints.

Understanding Access Control Lists

An access control list is a whitelist of users/groups whose endpoint(s) of a particular type are allowed to authenticate with the RealPresence Resource Manager system for provisioning and video network services. Access Control Lists can be used only with endpoints that are dynamically managed.

This is particularly useful when controlling Polycom’s soft endpoints such as RealPresence Desktop and RealPresence Mobile which use provisioning credentials to authenticate with your video network.

You can use Access Control Lists to control access to the RealPresence Resource Manager system for the following endpoint types:

- Polycom HDX systems
- Polycom RealPresence Group Series
- Polycom RealPresence Immersive Studio systems
- Polycom CMA Desktop
- RealPresence Desktop
- RealPresence Mobile (multiple device models)
- Polycom VVX systems
- Polycom CX
- RealPresence Debut
- RealPresence Centro

Planning Implementation of Access Control Lists

Once you create an Access Control List for an endpoint type, all users of that endpoint type must be included on an Access Control List in order to access the RealPresence Resource Manager system for provisioning and authentication.

In other words, if you create an Access Control List for an endpoint type and associate it with a user group, only those members of that user group can access the RealPresence Resource Manager system for provisioning and authentication.

If you do not create Access Control List for an endpoint type, then all users with that endpoint type are allowed to access the RealPresence Resource Manager for provisioning and authentication.
For example, if you create an **Access Control List** that includes RealPresence Mobile systems, all users of RealPresence Mobile endpoints must now be included on that **Access Control List** in order for their endpoints to be provisioned and authenticate with your video network.

However, if you have not created an Access Control List for HDX systems, all users with HDX systems managed by the RealPresence Resource Manager system can have their endpoints be dynamically managed.

**Plan Implementation of Access Control List**

It’s important to plan your implementation of Access Control Lists. Use the following steps:

1. Determine an endpoint type of which you want to limit RealPresence Resource Manager system access.
2. Determine which user groups you want to include in the Access Control List.

**Using Access Control Lists in a Multi-Tenancy Environment**

You can associate an **Access Control List** with a specific area.

If you associate the Access Control List with a user group that is not in the same area as the assigned area of the Access Control List, you will be prompted to allow the RealPresence Resource Manager system to change the area of the group to match the area of the list.

If you re-assign an Access Control List to a different area, you are prompt to allow the RealPresence Resource Manager system to change the area of the group(s) to match the area of the list.

User groups associated with an Access Area List must reside in the same area as the list.

**Add a New Access Control List**

You can create an Access Control List that includes all endpoints of a particular device type(s) within a user group. For example, you can create an Access Control List that enables all RealPresence Mobile users that belong to a particular group to access the RealPresence Resource Manager for provisioning.

Users with the administrator, device administrator or area administrator role can create Access Control Lists.

**To add a new Access Control List:**

1. Go to **Endpoint > Dynamic Management > Access Control Lists**. The **Access Control Lists** page appears.
2. Click **Add**.
3. In the **Add Access Control List** dialog box, complete the following fields in the General Info tab.
4. Click **Associate Endpoint Types**.
5. In the **Associated Endpoint Types** section, select and move the desired **Available Endpoint Types** endpoint types(s) to **Selected Endpoint Types** list.
6 When you include a RealPresence Mobile endpoint, you need to also choose the endpoint model to include in the Access Control List. In the Select the RealPresence Mobile device model section, select and move the desired endpoint models to the Selected Endpoint Model list. All endpoint models are included by default.

7 Click Associated User Groups.

8 Use the Search Group field to find the group(s) you want to associate with this Access Control List.

9 In the Search Results section, select and move the desired group(s) to Selected Groups list.

10 Click OK.

Edit an Access Control List

You can edit an Access Control List at any time. You can add or delete IP addresses or the groups associated with the list. When you alter an access control list, the changes take place immediately. Users with the administrator, device administrator or area administrator role can create Access Control Lists.

To edit an Access Control List:

1 Go to Endpoint > Dynamic Management > Access Control Lists. The Access Control Lists page appears.

2 Select an access control list.

3 Click Edit.

4 Modify any of the fields and click OK.

If you change the area of the access control list, you are asked to confirm that all groups associated with the list will also be changed to the new area.

Access Control List Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control List Name</td>
<td>Enter a unique name for the Access Control List.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the Access Control List.</td>
</tr>
<tr>
<td>Assign Area</td>
<td>If areas are enabled, and you have permission to manage more than one area, use the Assign Area drop-down list to assign the Access Control List to an area. The drop-down list does not appear if areas are not enabled or the user does not have permission to assign an area.</td>
</tr>
</tbody>
</table>
Delete an Access Control List

You can delete an access control list. Deleting an access control list may deny user groups associated with the list access to RealPresence Resource Manager conferencing services. Remember to reassign any user groups to a new access control list if you need them to continue to be able to authenticate.

Users with the administrator, device administrator or area administrator role can create Access Control Lists.

To delete an access control list:

1. Go to Endpoint > Dynamic Management > Access Control Lists.
   The Access Control Lists page appears.

2. Select an access control list.

3. Click Delete.

4. Click OK to confirm the deletion.
Scheduling Endpoint Software Updates

The Polycom RealPresence Resource Manager system’s 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: dynamic and scheduled. Dynamic and scheduled software update are exclusive endpoint management scenarios. Endpoints enabled for dynamic 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.

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 dynamic 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.

Creating Scheduled Software Updates for Endpoints

To implement scheduled software updates, you must first create respective software updates for your endpoints.

Only users with the Administrator role can create software updates.
List the Serial Numbers for the Endpoints to be Updated

You need to create a text file that contain the list of endpoints to be updated.
Only users with the Administrator role can create software updates.

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

1. Go to Endpoint > Scheduled Management > Upload Software Updates.
2. Select the endpoint type for which to get serial numbers.
   - If getting serial numbers for a scheduled update, select the appropriate Endpoint Type and Endpoint Model combination for the endpoint to update. You can select more than one Endpoint.
   - If getting serial numbers for a dynamic software update, click the appropriate tab for the endpoint.
3. Click Get Serial Numbers from the More menu.
   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>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.
6. Click Get Serial Numbers from the More menu.
   The serial number(s) appear in the text box on the page.
7. Create a .txt file containing the serial number(s).
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.

82071007E1DACD
82070407E010CD
820418048078B2
82040903E00FB0

b. Save the .txt file.

c. Return to the endpoint serial number list and click Close.

The Software Updates list reappears.

8. Repeat from step 2 to step 7 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.

9. Click Close.

The Software Updates list reappears.

Download the Required Software Package

You need to download the required software packages to update the software.

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:
   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.

Upload the Software Update for Scheduled Software Updates

Polycom recommends you to do software updates using the split packages available on Polycom’s support website to reduce system resource consuming.

Only users with the Administrator role can create software updates.

To upload the software package and create a software update profile:

1. Go to Endpoints > Scheduled Management > Upload Software Updates.
Scheduling Endpoint Software Updates

2. Select an endpoint type to update.
3. Click **Add**.
4. In the **Upload Software Update** dialog, verify the endpoint type and model.
5. 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 Requesting Update Activation).

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 downloaded.
7. Enter a meaningful description that will help other users to understand the purpose of the software update.
8. Click **OK**.

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

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 canceled.
- 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.

Supported Endpoints for Scheduled Software Updates

Scheduled software updates are available for these endpoint types:

- HDX Series—when operating in scheduled management mode (not using a provisioning server)
- LifeSize
- Cisco T150
- Cisco C-Series
- Cisco SX-Series
- Cisco EX-Series
• Cisco MX-Series
• Cisco 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 Management > Schedule Software Updates**.
2. As needed, click **Filter** to filter the endpoint list.
3. Select the endpoints of interest and click **Software Update** from the **More** menu.
4. In the **Schedule Software Update** dialog, 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.
   c. 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>

**Caution:** 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 **Scheduled Software Update**, 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 scheduled software update.
Endpoint List in the Scheduled Software Update View

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Filter choices for this view include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Endpoint Type</strong>—Filters the list by endpoint type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Endpoint Name</strong>—Searches the list by the endpoint’s system name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong>—Searches the list by endpoint’s IP address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ISDN Video Number</strong>—Searches the list by endpoint’s ISDN video number.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alias</strong>—Searches the list by endpoint’s alias.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Site</strong>—Searches the list by site location.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Area</strong>—Filters the endpoint list by area. This filter is only available when areas are enabled and when the user manages more than one area.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the endpoint’s last scheduled software update. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Failed</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Clear</strong></td>
</tr>
<tr>
<td>Name</td>
<td>The system name of the endpoint.</td>
</tr>
<tr>
<td>Model</td>
<td>The type of endpoint. Scheduled software update is only available for these endpoint types:</td>
</tr>
<tr>
<td></td>
<td>• <strong>HDX Series</strong>—when operating in scheduled management mode (not using a provisioning server)</td>
</tr>
<tr>
<td></td>
<td>• <strong>QDX Series</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>LifeSize</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Cisco T150</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Cisco C-Series</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Cisco SX-Series</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Cisco EX-Series</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Cisco MX-Series</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Cisco MXP series</strong></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the endpoint.</td>
</tr>
<tr>
<td>Current Version</td>
<td>The version of software installed during the last successful software update procedure.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>When the endpoint is scheduled for software update, this field shows the date and time for the scheduled software update process.</td>
</tr>
</tbody>
</table>

Scheduled Software Update Actions

Besides providing access to the endpoint views, you can perform the following actions:
Scheduling Endpoint Software Updates

For information about these endpoint actions, see Scheduling Endpoint Software Updates.

**View Scheduled Software Update Information**

You can view software update information for endpoints that are scheduled eligible for scheduled software updates.

To view information about scheduled software updates:

1. Go to Endpoint > Scheduled Management > Schedule Software Update.
2. As needed, click Filter to filter the endpoint list. Filter choices include Endpoint Type, Endpoint Name, IP Address, ISDN Video Number, Dial String, and Site.
3. Select the endpoint of interest.
4. Click View Details to open the Endpoint Summary pane, expand the Software Update Details tab.

**View List of Software Update Packages**

You can view a list of endpoints eligible for software updates.

To view the list of scheduled software update packages:

» Go to Endpoint> Scheduled Management > Upload Software Updates.

The Upload 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.

To cancel scheduled software updates:

1. Go to Endpoint > Scheduled Management > Schedule Software Updates.
2. As needed, click Filter to customize the endpoint list.

---

<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 Clear state.</td>
</tr>
</tbody>
</table>

---

For information about these endpoint actions, see Scheduling Endpoint Software Updates.
3 Select the endpoint or endpoints of interest and click **Cancel Update** from the *More* menu.

   A confirmation dialog appears. The dialog 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 a operational state.
Dynamic Provisioning of Endpoints for SIP Server Integration

The RealPresence Resource Manager system enables you to dynamically provision some Polycom endpoints with the SIP server integration information with the SIP credentials and SIP settings the endpoints need.

SIP settings can only be provisioned when you use dynamic management. You can provision SIP by using both a Network provisioning profile and an Admin Config provisioning profile. You cannot use scheduled or bundled provisioning to provision SIP settings.

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 Skype For Business
- BroadSoft BroadWorks
- Polycom RealPresence DMA system
- Siemens OpenScape
- Avaya Aura Session Manager
- Cisco Unified Communications Manager

You need to consider the following items when using SIP provisioning:

- SIP settings are configured using network provisioning profiles.
- 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 ensure that users have existing SIP URIs before provisioning SIP settings.
- Provisioning Microsoft SIP.

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, ensure that each user has an existing SIP URI before you can use Network provisioning profiles to provision SIP settings.

Provisioning 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 ensure that users have SIP URIs.

Create Authentication Information for SIP Endpoints

To have the RealPresence Resource Manager system dynamically 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 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.
2. Import SIP URI data for those users.

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.

To import SIP URI data:

1. Create a CSV file in the format described here. The import requires a CSV file in the following format:
   
   domain,username,deviceType,SIPURI,devicename
   
   where:
Dynamic Provisioning of Endpoints for SIP Server Integration

- **domain**—Specifies the domain the user uses to log in to the RealPresence Resource Manager system.
- **username**—Specifies the RealPresence Resource Manager system user name.
- **deviceType**—Specifies the device type (valid values are HDX, VVX, CMA Desktop, RPMobile, RP Desktop, GroupSeries or All_Types).
- **SIP URI**—Specifies the SIP URI for this user.

For example, this import reserves the SIP URI johndoe@example.com for all device types for the John Doe user:

`local,johndoe,All_Types,johndoe@example.com`

1. From the RealPresence Resource Manager system, go to **User > Users**.
2. Go to **More > Import User Aliases**.
3. Navigate to the CSV file, select it, and click **Open**.

### Editing SIP URI Data

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.

You can edit SIP URI data in either of the following ways:

- Upload a CSV file that has changes or new data. Data in the CSV file is added to any existing data.
- 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.

### Provision SIP Settings for SIP Server Integration

SIP settings are dynamically provisioned with a network provisioning profile. This procedure describes how to change existing network provisioning settings so that they provision integration with a SIP server.

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 **Endpoint > Dynamic Management > Provisioning Profiles**.
2. Select the **Network Provisioning Profile** you want to edit and click **/**.
3. In the **Edit Profile** dialog, click **SIP Settings** and select these options.

<table>
<thead>
<tr>
<th>Fields</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</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>Backup Proxy Server</td>
<td>Specify the IP address or DNS name of a backup proxy server for the network.</td>
</tr>
</tbody>
</table>
Dynamic Provisioning of Endpoints for SIP Server Integration

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 a Microsoft Office Communications Server 2007 or Microsoft Skype For Business Server 2010 environment, specify the IP address or DNS name of the Office Communications Server or Skype For Business Server server.</td>
</tr>
<tr>
<td></td>
<td>• If register a remote HDX system with an Office Communications Server Edge Server or Skype For Business Server Edge Server, use the fully qualified domain name of the access edge server role.</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></td>
<td>• Auto enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments.</td>
</tr>
<tr>
<td></td>
<td>• TCP provides reliable transport via TCP for SIP signaling.</td>
</tr>
<tr>
<td></td>
<td>• UDP provides best-effort transport via UDP for SIP signaling.</td>
</tr>
<tr>
<td></td>
<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.</td>
</tr>
<tr>
<td></td>
<td>When you choose this setting, the system ignores TCP/UDP port 5060.</td>
</tr>
<tr>
<td>Server Type</td>
<td>Specify the SIP server type.</td>
</tr>
<tr>
<td></td>
<td>• Standard:</td>
</tr>
<tr>
<td></td>
<td>• Polycom:</td>
</tr>
<tr>
<td></td>
<td>• Avaya:</td>
</tr>
<tr>
<td></td>
<td>• BroadSoft:</td>
</tr>
<tr>
<td></td>
<td>• Cisco:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft: If you are integrating with a Microsoft Server, you must also provision a group for the endpoint, see Provision Group for Microsoft Skype For Business or Microsoft Office Communications Server Integration.</td>
</tr>
<tr>
<td></td>
<td>• Siemens:</td>
</tr>
<tr>
<td>Verify Certificate</td>
<td>Enable this option when the endpoint system’s certificate should be verified by the certificate authority.</td>
</tr>
<tr>
<td>Use Endpoint Provisioning</td>
<td>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.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Common SIP User Name</td>
</tr>
<tr>
<td></td>
<td>Specify the name to use for authentication when registering with a SIP registrar server, for example, <a href="mailto:msmith@company.com">msmith@company.com</a>. If the SIP proxy requires authentication, this field and the password cannot be blank.</td>
</tr>
<tr>
<td>Use Enterprise URI</td>
<td>Enable this option with the endpoint should use the SIP URI of the enterprise user (domain user).</td>
</tr>
<tr>
<td>Common SIP Password</td>
<td>Specify the password that authenticates the system to the registrar server.</td>
</tr>
</tbody>
</table>

4 Click **OK**.

5 You need to ensure that you have created a provisioning rule that applies this network provisioning profile to the intended site and endpoints.
Dynamic Provisioning of Endpoints for SIP Server Integration

Related Topics
Provision Group for Microsoft Skype For Business or Microsoft Office Communications Server Integration

Provision Group for Microsoft Skype For Business or Microsoft Office Communications Server Integration

You must set up the Microsoft Skype For Business or Office Communications Server group that needs to be provisioned to endpoints in each Admin Config provisioning profile. This controls the directory that endpoints can see.

You cannot provision integration with a Microsoft Skype For Business or Office Communications Server via scheduled provisioning. If the endpoint being provisioned is not capable of integration with a Microsoft Skype For Business or Office Communications Server, the endpoint will ignore this setting. The group setting here applies to both Microsoft Skype For Business and Office Communication Server.

To provision integration with Microsoft Skype For Business or Office Communications Server:

1. Go to Endpoint > Dynamic Management > Provisioning Profiles.
2. Select an Admin Config profile of interest and click Edit .
3. Click Microsoft Skype For Business Settings and enter a Group Name.
   The Group Name is the group set in the Microsoft Skype For Business Server or Office Communication Server.
4. Click OK.

Microsoft Directory Considerations

When Polycom endpoints are registered with a Microsoft Skype For Business 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.

Using Machine Accounts

For dynamically managed endpoints associated with a room, a user assigned the Administrator role must associate each room in the RealPresence Resource Manager system with a machine account. In addition, dynamically managed HDX systems and RealPresence Group Series require machine accounts.
The machine account enables the endpoint to connect and authenticate with the RealPresence Resource Manager system for directory and dynamic management purposes without using the endpoint user’s account. You should use a unique machine account for each room or endpoint you need to provision.

You can set up 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.
- If your system is integrated with Active Directory and you want to associate a machine account with an Active Directory account, you must first create that account in Active Directory.

**Add a Machine Account**

When you add a machine account, you must associate it with a user or a room. You can choose to use an existing user or room or create one when you add the machine account.

Once you have created this machine account on the RealPresence Resource Manager system, provide this information to the appropriate endpoint administrator. They should enter this User ID and Password as the User Name and Password on the Provisioning Service page.

Note that the machine account password expires after one year. After the expiration, the endpoint 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:**

2. Click Add.
3. In the Add Machine Account dialog, complete the fields.
4. Click OK.

**Related Topics**

- Machine Account Fields

**Edit a Machine Account**

You can edit a machine account. Once you have created this machine account on the RealPresence Resource Manager system, provide this information to the appropriate endpoint administrator. They should enter this User ID and Password as the User Name and Password on the Provisioning Service page.

Note that the machine account password expires after one year. After the expiration, the endpoint 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 edit a machine account:

2. Select a machine account and click Edit.
3. In the Edit Machine Account dialog, edit the fields as needed.
4. Click OK.

**Machine Account Fields**

<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. This option can only create a local room account. If you want to associate a machine account with an Active Directory account, you must first add the account through Active Directory.</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>
Using Zero-Touch Provisioning

After configuring Zero-Touch provisioning from the RealPresence Resource Manager system, an endpoint can be provisioned automatically. Because dynamic provisioning rules are used to apply provisioning profiles, you must ensure that endpoints are associated with room or user accounts before provisioning can take place. You can do this automatically by configuring your settings or by manually associating an endpoint with a room or user account.

Only RealPresence Debut support Zero-Touch provisioning. The RealPresence Debut can connect to the network via DHCP and if it can find the RealPresence Resource Manager system, it will dynamically be provisioned according to any dynamic provisioning rules and profiles you have created.

Configure your DHCP Server

Configure your DHCP server to be aware of the RealPresence Resource Manager system’s IP address, if you wish it to resolve queries for the RealPresence Resource Manager by the RealPresence Resource Manager’s host name or IP address.

You can use the default available option of “066 Boot Server Host Name” or add a custom option.

If you choose to use a custom option, you need to update the provisioning page of the RealPresence Debut system. See the RealPresence Debut System Administrator’s Guide for more information.

To configure your DHCP server:

1. Login to the DHCP server and navigate to the Server Options page.
2. Find the default Available Option 066 Boot Server Host Name and add the string value of the RealPresence Resource Manager system’s IP address. The default format is https://<user>:<password>@ip_address.

Configure Zero Touch Provisioning Settings

In order to be provisioned by zero-touch provisioning, an endpoint must be associated with a room or user account. You can configure your system to automatically create this account when the endpoint auto-discovers the RealPresence Resource Manager system via DNS.

The automatic association you configure cannot create accounts in an enterprise directory. If you want to associate provisioned endpoints with enterprise room or user accounts, you need to make the association manually.

To configure Zero Touch Provisioning Settings:

2 Click **Zero Touch Provisioning Settings**.
3 In the Settings dialog, mark the **autoGenerate** check box.
4 In the **Default Language** drop-down list, select a language to use.
5 Click **OK**.

**Manually Associate an Endpoint with a Room or User**

To take advantage of zero touch provisioning, you must ensure that each endpoint is associated with a room or user account. You can also manually associate the endpoint with an existing account if you did not configure your system to automatically create this account when the endpoint auto-discovers the RealPresence Resource Manager system via DHCP.

Alternatively, you can set up the RealPresence Resource Manager system to automatically add a room account (and the associated machine account) when an endpoint discovers the RealPresence Resource Manager system via DHCP.

**To associate an endpoint with a room or user:**

1. Go to **Endpoints > Dynamic Management > Zero Touch Provisioning Bindings**.
2. Click **Add**.
3. Enter the serial number of the RealPresence Debut system you want to provision.
4. Select a room or user to associate with the endpoint.
   a. Click **Select**.
   b. Click **Filter**.
   c. In the **Search Users and Rooms** 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. You must be logged into the system as an enterprise user in order to search for enterprise users.
   d. Select the user to associate and click **OK**.
5. In the **Add** dialog, click **OK**.
6. If there is not a machine account already associated with the user you selected, you are prompted to create one.

**Related Topics**

Add a Machine Account

**Enable Calendaring Service**

In order for the RealPresence Debut to use the calendaring feature, it must use an Active Directory credentials to communicate with the RealPresence Resource Manager system.
After the initial zero-touch provisioning, you must log in to the RealPresence Debut system's administrator interface to change the account used for provisioning to an Active Directory account.

See the RealPresence Debut System Administrator Guide for more details.
Dynamically Managing a RealPresence Access Director System

The RealPresence Resource Manager system enables you to dynamically manage a RealPresence Access Director system.

You can use a RealPresence Access Director server provisioning profile to dynamically manage the RealPresence Access Director system and configure it with the right network information to allow for firewall traversal in your video infrastructure environment.

Creating a Site for the RealPresence Access Director System

You should create a site that includes the subnet on which the RealPresence Access Director resides. You’ll need to add the RealPresence Access Director system’s internal IP to the subnet of the site.

You cannot use the same site for more than one RealPresence Access Director system. You must create a unique site for each RealPresence Access Director system that you use.

Create a RealPresence Access Director Server Provisioning Profile

You can dynamically provision a RealPresence Access Director system with the RealPresence Access Director server provisioning profile.

A RealPresence Access Director server provisioning profile includes all applicable settings for a RealPresence Access Director system.

The RealPresence Access Director system should be configured with the IP addresses of the Polycom RealPresence DMA system as the gatekeeper and the SIP server within your environment.

With RealPresence Access Director server provisioning profiles, you can ensure that an RealPresence Access Director system has the optimal and correct firewall traversal settings to support endpoints that will depend on it for firewall traversal.

As soon as an RealPresence Access Director system is configured to use the RealPresence Resource Manager for its provisioning server, it starts polling for provisioning profile updates. To ensure out-of-box usability, the RealPresence RealPresence Resource Manager system comes with a default RealPresence Access Director Server provisioning profile.
The default RealPresence Access Director server provisioning profile cannot be associated with any provisioning rules. You must add a new RealPresence Access Director server provisioning profile in order to customize the settings of your RealPresence Access Director system.

**To create a RealPresence Access Director provisioning profile:**

1. Go to Endpoint > Dynamic Management > RPAD Server Provisioning Profiles.
2. Click Add.
3. In the General Info section of the Add New Profile section,
   - Enter a name for the new RealPresence Access Director server provisioning profile.
   - Select Server Provisioning Profile from the drop-down list.
4. As needed, edit the server provisioning details and click Apply.
5. Click OK.

**Related Topics**

Available Settings for RealPresence Access Director Server Provisioning Profile

**Creating a Network Provisioning Profile for Endpoints**

You need to create a network provisioning profile to apply to all dynamically managed endpoints within the same site as a RealPresence Access Director system. These endpoints need to be provisioned to use the RealPresence Access Director system external IP address for all of their network settings.

Ensure that all network settings (gatekeeper, presence server, SIP server, and directory) are set to the external IP address of the RealPresence Access Director system.

For example, instead of the IP address of the RealPresence DMA system’s gatekeeper, provision endpoints to use the external IP address of the RealPresence Access Director system as the gatekeeper IP.

**Related Topics**

Network Provisioning Profiles

**Creating an Admin Config Provisioning Profile**

If you want to provision the endpoints that use the RealPresence Access Director system with specific admin configuration settings, you can create an Admin Config profile to use.

**Related Topics**

Admin Config Provisioning Profiles
Creating a Provisioning Rule and Associate it with All Related Profiles

You need to create a provisioning rule that includes a condition that defines the rule to be applied to the site that includes the RealPresence Access Director system.

For example, \((\text{Site.Site} = \text{RealPresence Access Director Site})\)

At a minimum, the provisioning rule must contain this site condition.

Associate both the **RealPresence Access Director Server Provisioning** profile and the **Network Provisioning** profile (for endpoints) with the rule. You can also include an **Admin Config** profile if needed. This ensures that all endpoints within the subnet of the site created for the RealPresence Access Director are provisioned with the correct settings. It also provisions the RealPresence Access Director system.

Related Topics

Creating Dynamic Provisioning Rules

Creating a User Account for the RealPresence Access Director System

You need to create a user account for RealPresence Access Director system in order to authenticate with the RealPresence Resource Manager system’s provisioning service.

Use this account to register the RealPresence Access Director system with the RealPresence Resource Manager system’s provisioning service.

See the *Polycom RealPresence Access Director System Administrator’s Guide* for more information about provisioning the RealPresence Access Director system.

Available Settings for RealPresence Access Director Server Provisioning Profile

This table lists the RealPresence Access Director settings that can be provisioned.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RPAD Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Time Server</td>
<td>Specify whether to connect to a time server for automatic system time settings. Currently, the RealPresence Access Director system can be provisioned only with a <strong>Manual</strong> setting. If you use the <strong>Auto</strong> setting, the RealPresence Access Director system will behave as if the Time Server is set to <strong>Off</strong>. Select <strong>Manual</strong> to require that the RealPresence Access Director 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 <strong>Time Server Address</strong> field. If <strong>Time Server</strong> is set to <strong>Off</strong>, or if the <strong>Time Server</strong> is set to <strong>Manual</strong> but the endpoint system cannot connect to the time server, the date and time must be manually reset at the endpoint.</td>
</tr>
<tr>
<td>Primary Time Server Address</td>
<td>Specify the address of the primary time server when <strong>Time Server</strong> is set to <strong>Manual</strong>.</td>
</tr>
<tr>
<td>Secondary Time Server Address</td>
<td>Specify the address of the secondary time server when <strong>Time Server</strong> is set to <strong>Manual</strong>.</td>
</tr>
<tr>
<td>Provisioning Polling Interval</td>
<td>Specify the frequency at which the RealPresence Access Director system polls the RealPresence 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.</td>
</tr>
<tr>
<td>Heartbeat Posting Interval</td>
<td>Specify the frequency at which the RealPresence Access Director system poll the RealPresence Resource Manager system for a heartbeat.</td>
</tr>
<tr>
<td><strong>Server Status Posting Interval</strong></td>
<td></td>
</tr>
<tr>
<td><strong>RPAD Settings 2</strong></td>
<td></td>
</tr>
<tr>
<td>Enable IP H.323</td>
<td>Configure the system to enable or disable H.323 signal forwarding.</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. The IP address of the internal gatekeeper that the system forwards to when endpoints behind the system send gatekeeper registration or H.323 call requests.</td>
</tr>
<tr>
<td>Enable SIP</td>
<td>Specify whether to enable SIP calls and enable the provisioning of SIP settings. Configures the system to enable or disable SIP signal forwarding.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Specify the IP address or DNS name of the internal SIP proxy server that the system forwards to when endpoints behind the system send SIP call requests. Enter the RealPresence DMA signaling IP address in this field.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Specify the IP address or DNS name of the internal SIP registrar server that the system forwards to when endpoints behind the system send SIP registration requests. Enter the RealPresence DMA signaling IP address in this field.</td>
</tr>
<tr>
<td>Use Default Directory Server</td>
<td>Not provisionable in RealPresence Resource Manager system v8.2.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Server</td>
<td>Not provisionable in RealPresence Resource Manager system v8.2.</td>
</tr>
<tr>
<td>Presence Server</td>
<td>Not provisionable in RealPresence Resource Manager system v8.2.</td>
</tr>
<tr>
<td>Verify Certificate</td>
<td>Enable this option when the RealPresence Access Director system's certificate should be verified by the certificate authority.</td>
</tr>
</tbody>
</table>
Phone Management

The RealPresence Resource Manager system can be used as a central provisioning server for supported phones.
Managing Phones

The RealPresence Resource Manager system can be used as a central provisioning server for supported phones. When a phone is provisioned, it polls the RealPresence Resource Manager system for configuration profile settings and software updates at intervals that you define. You can remotely control the configuration settings and software version of the phone, according to the conditions that you define. The RealPresence Resource Manager system communicates with phones via HTTP or HTTPS.

Polycom recommends you to use the HTTPS protocol, especially when managing over 400 phones to enhance the performance.

Overview of Phone Management Setup

Setting up phone management is a multi-step process that may include the following tasks:

- Adding phones to the RealPresence Resource Manager system.
- Setting up configuration profiles.
- Deploying configuration profiles to phones per conditions.
- Setting up software updates.
- Registering phones to a SIP server.
- Setting up phone management settings.

Supported Phones and Call Servers

RealPresence Resource Manager supports standard SIP servers and the following Polycom phones:

Polycom CX5100 does not support sync messages from the RealPresence Resource Manager system. For example, after making changes to a configuration profile applied to CX5100 endpoints, and click **Save and Apply** to apply the changes immediately, CX5100 cannot respond and reboot to accept the changes. The changes take effect at the next polling interval. You also can manually reboot CX5100 to apply the changes.
### Supported Phones Types and Models

<table>
<thead>
<tr>
<th>Phone Type</th>
<th>Phone Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVX</td>
<td>VVX 101</td>
</tr>
<tr>
<td></td>
<td>VVX 150</td>
</tr>
<tr>
<td></td>
<td>VVX 201</td>
</tr>
<tr>
<td></td>
<td>VVX 250</td>
</tr>
<tr>
<td></td>
<td>VVX 300</td>
</tr>
<tr>
<td></td>
<td>VVX 301</td>
</tr>
<tr>
<td></td>
<td>VVX 310</td>
</tr>
<tr>
<td></td>
<td>VVX 311</td>
</tr>
<tr>
<td></td>
<td>VVX 350</td>
</tr>
<tr>
<td></td>
<td>VVX 400</td>
</tr>
<tr>
<td></td>
<td>VVX 401</td>
</tr>
<tr>
<td></td>
<td>VVX 410</td>
</tr>
<tr>
<td></td>
<td>VVX 411</td>
</tr>
<tr>
<td></td>
<td>VVX 450</td>
</tr>
<tr>
<td></td>
<td>VVX 500</td>
</tr>
<tr>
<td></td>
<td>VVX 501</td>
</tr>
<tr>
<td></td>
<td>VVX 600</td>
</tr>
<tr>
<td></td>
<td>VVX 601</td>
</tr>
<tr>
<td></td>
<td>VVX 1500</td>
</tr>
<tr>
<td>SoundStation</td>
<td>SoundStation IP 5000</td>
</tr>
<tr>
<td></td>
<td>SoundStation IP 6000</td>
</tr>
<tr>
<td></td>
<td>SoundStation IP 7000</td>
</tr>
<tr>
<td></td>
<td>SoundStation Duo</td>
</tr>
<tr>
<td>SoundPoint</td>
<td>SoundPoint IP 321</td>
</tr>
<tr>
<td></td>
<td>SoundPoint IP 331</td>
</tr>
<tr>
<td></td>
<td>SoundPoint IP 335</td>
</tr>
<tr>
<td></td>
<td>SoundPoint IP 450</td>
</tr>
<tr>
<td></td>
<td>SoundPoint IP 550</td>
</tr>
<tr>
<td></td>
<td>SoundPoint IP 560</td>
</tr>
<tr>
<td></td>
<td>SoundPoint IP 650</td>
</tr>
<tr>
<td></td>
<td>SoundPoint IP 670</td>
</tr>
<tr>
<td>SoundStructure VoIP Interface</td>
<td>SoundStructure VoIP Interface</td>
</tr>
<tr>
<td>Polycom Trio</td>
<td>Polycom Trio 8500</td>
</tr>
<tr>
<td></td>
<td>Polycom Trio 8800</td>
</tr>
<tr>
<td></td>
<td>Polycom Trio Visual+</td>
</tr>
</tbody>
</table>
Managing Phones

Phones can be added to the RealPresence Resource Manager system via the following ways:

- Adding phones automatically
- Adding phones manually
- Adding phones by importing a CSV file
- Adding phones by syncing with a CUCM server

All the added phones can be monitored and managed from the **Endpoint > Monitor View** page. From this page, you can:

- View phone’s information
- View phone’s detail information
- Edit a Phone
- Upload Phone Configuration Files
- Delete a Phone
- Reboot phones
- Go to phone’s Web GUI
- Set Active Directory Password
- Control Call Remotely
- Monitor Phones Behind Firewall

**Related Topics**

- View the Endpoint List
- View Endpoint Details
- Edit a Phone
- Upload Phone Configuration Files
- Delete a Phone
- Reboot an Endpoint
- Manage an Endpoint
- Set Active Directory Password

## Supported Phones Types and Models

<table>
<thead>
<tr>
<th>Phone Type</th>
<th>Phone Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence Group Series</td>
<td>(Hardware version 20 and later)</td>
</tr>
<tr>
<td></td>
<td>RealPresence Group 310</td>
</tr>
<tr>
<td></td>
<td>RealPresence Group 500</td>
</tr>
<tr>
<td>CX</td>
<td>CX5100</td>
</tr>
<tr>
<td></td>
<td>CXPhone5500</td>
</tr>
</tbody>
</table>

Polycom, Inc.
Managing Phones

Control Call Remotely
Monitor Phones Behind Firewall

**Automatically Added Phones**

Phones connected via Intranet can be added to the RealPresence Resource Manager system automatically via the HTTP/HTTPS protocol.

Phones behind a firewall, Polycom recommends you to use HTTPS to connect to a RealPresence Resource Manager system.

When a phone is online and connects to the RealPresence Resource Manager system, the phone is provisioned by the system.

You can find automatically added phones by viewing the **Mode Auto-added Phones** information on the **Endpoint > Monitor View** page.

When a phone is automatically added to the RealPresence Resource Manager system and then the same phone (with the same MAC address) is synced from CUCM, the phone becomes a synced CUCM phone. If this phone is removed from CUCM, it is also removed from the RealPresence Resource Manager system.

**Configure Automatically Added Phones for Provisioning**

To use the RealPresence Resource Manager system as phones’ provisioning service, you usually need to configure some settings via the phone’s web interface.

**To configure automatically added phones for provisioning:**

- Select HTTP or HTTPS as the transport protocol for phones using the Intranet. Select HTTPS as the transport protocol for phones behind firewall.
- When selecting HTTPS, you need a public certificate installed on the RealPresence Resource Manager system for HTTPS to work without loading the private CA, or you can disable the Common Name Validation on the phone as the self-signed certificate is trusted by the phones.
- Specify the RealPresence Resource Manager system address in the following formats:
  - `RPRM_Address`
  - `RPRM_Address/phoneservice/configfiles`
  For example, your RealPresence Resource Manager system address is 172.21.125.243. You need to use "172.21.125.243" or "172.21.125.243/phoneservice/configfiles" as the server address.
- Specify the provisioning account and password configured on the **Endpoint > Phone Management > Phone Management Setting** page. See Configure Your Phone Management Settings for details.

The way to configure RealPresence Trio Visual+ is different from other phones. Please refer to the **Polycom RealPresence Trio User Guide** for more information.

**Related Topics**

Configure Your Phone Management Settings
Editing Automatically Added Phones

After a phone is discovered and added to the RealPresence Resource Manager system, a user with the device administrator role can edit its settings. After manually editing an auto-added phone, the mode of this phone will become **Manually Added Phones**.

For information on editing automatically added phones, see Edit a Phone for details. You also can export all the auto-added phones to a CSV file, edit phones information in a batch, and then import the CSV into the RealPresence Resource Manager system. See Export and Edit Phones on how to edit phones in a CSV file.

**Related Topics**
- Edit a Phone
- Export and Edit Phones

Add a Phone Manually

Phones can be added one by one on the **Endpoint > Monitor View** page.

To add a phone to the system:

1. Go to **Endpoint > Monitor View** and click **Add**.
2. In the **Add New Endpoint** dialog, select phone type that you want to add in the **Endpoint Type** drop-down list.
3. Specify the MAC address and the system name of the phone.
4. In the **Line Address** tab, click **Add** to add line information by specifying **SIP URI**, **Display Name**, **Digest Account**, and **Digest Password** if needed in the **Lines Information** dialog.
5. (Optional) On the **Endpoint Group Association** tab, select the endpoint group to associate with and click **Add**.
   - Click the arrow icon to adjust the priority of endpoint groups. The arrow icons appear when the cursor stays on an endpoint group.
   - See Working with Endpoint Groups for details about endpoint group.
6. (Optional) On the **Configuration Profile Association** tab, select the configuration profile to associate with and click **Add**.
   - Click the arrow icon to adjust the priority of configuration profiles. The configuration profiles set on device level always has higher priority.
   - See Working with Phone Configuration Profiles for details on configuration profile.
7. Click **OK**.

**Related Topics**
- Working with Endpoint Groups
- Working with Phone Configuration Profiles
**Edit a Phone**

You can edit manually added, automatically added, or imported phones.

Polycom does not recommend that you change the line information of CUCM synced phones from the RealPresence Resource Manager system since the changes will be overwritten at the next CUCM sync interval.

To edit a phone:

1. Go to Endpoint > Monitor View.
2. Click Filter, select Mode, and select one of the following modes to filter phones that you want to edit:
   - Auto-added Phones
   - Manually Added Phones
3. Select a phone and click Edit.
4. Edit the phone and line information as needed.
   

   All the line information is listed in the Line Address tab.

   **Provisioning Line** indicates how this line is created. If the line is created from phones, **Provisioning Line** is False. If the line is created by RealPresence Resource Manager admin, **Provisioning Line** is True.

   If you change the line information of an auto-added phone, the **Provisioning Line** value will change from False to True.

5. Do one of the following:
   - Click Save and Apply to apply the changes including the line information and configuration profiles changes to the online phone now. This operation may reboot the phone. This operation only applies this time changes to the phones. It does not apply previous changes to the phones. If the phone is offline or the phone is behind firewall, **Apply** is not displayed.
   - Click Save to wait for the updates to take effect at the next polling interval.

**Viewing Phone’s Status**

For internal phones, which the RealPresence Resource Manager system can connect to, the system sends API calls to phones as heartbeat messages to check if phones are online or offline. The interval is a random time between 5 to 10 minutes if there is no message from phones during the last intervals.

For external phones, which the RealPresence Resource Manager system cannot connect to via API calls, the offline detecting window is based on the configured provisioning polling interval plus 5 minutes. For example, if the polling interval is one hour, the RealPresence Resource Manager system will treat phones as offline if there is no message from phones in the past 65 minutes.

**Related Topics**

View the Endpoint List
**Upload Phone Configuration Files**

When uploading phone configuration files, you must upload the files to the correct directory, based on the purpose of the files.

The system supports CFG, XML, CSV, PEM, CRT, and CER file types and the following directories:

- MISC FILES
- CONTACTS DIRECTORY
- OVERRIDES DIRECTORY
- LICENSE DIRECTORY
- USER PROFILES DIRECTORY
- CERTIFICATE DIRECTORY
- FLK DIRECTORY

See the *Polycom UC Software Administrator Guide* for details on the directories.

To upload phone configuration files:

1. Go to **Endpoint > Monitor View**.
2. Select a phone.
3. Click **MORE > Upload Phone File**.
4. Select a file directory.
5. Browse and select a supported file.
6. Click **OK**.
7. After you upload the files, click **View Details** to display the phone’s detail information. The **Others** section contains these files.

**Change Endpoint Group Association**

When you edit a phone, you can associate it with an endpoint group, delete its association with an endpoint group, or prioritize multiple associated endpoint groups.

To change the association from a phone to an endpoint group:

1. Go to **Endpoint > Monitor View**.
2. Click the endpoint name that you want to edit from the **Endpoint Name** column.
3. In the **Edit Device** dialog box, click the **Endpoint Group Association** tab.
   
   - To associate the endpoint to an endpoint group, select the name of the endpoint group from the drop-down list and click **Add**.
   
   - To delete the association, click **Delete** at the right end of each line of the endpoint group list.
   
   - To prioritize an association, click the **Arrow** buttons to deprioritize or prioritize it, or give it the lowest or highest priority.
4. Click **Save and Apply** or **Save**.
Change Configuration Profile Association of Phones

When you edit a phone, you can associate it with a configuration profile, delete its association with a configuration profile, or prioritize multiple associated configuration profiles.

To change the association between phone and configuration profile:

1. Go to Endpoint > Monitor View.
2. Click the phone’s name that you want to edit from the Endpoint Name column.
3. In the Edit Endpoint dialog box, click the Configuration Profile Association tab.
   - To associate the phone to a configuration profile, select the profile’s name from the drop-down list and click Save and Apply.
   - To delete the association, click Delete at the right end of each line of the configuration profiles list.
   - To prioritize an association, click the Arrow buttons to deprioritize or prioritize it, or give it the lowest or highest priority.
4. Do one of the following:
   - Click Save and Apply to apply the configuration profiles changes to the online phone now. This operation may reboot the phone. This operation only applies this time changes to the phones. It does not apply previous changes to the phones.
     - If the phone is offline or the phone is behind firewall, Save and Apply is not displayed.
   - Click Save to wait for the updates to take effect at the next polling interval.

Delete a Phone

You can only delete manually added or imported phones. Phones synced from the Cisco Unified Communications Manager system cannot be deleted manually.

To delete a phone:

1. Go to Endpoint > Monitor View.
2. Select a manually added phone.
3. Click Delete.
4. Click Delete to confirm the deletion.

Set Active Directory Password

You can set an Active Directory password to the phones that are provisioned by the RealPresence Resource Manager system.

You can only set an Active Directory password for Polycom phones that support REST API, such as RealPresence Trio and Polycom VVX phones.
Managing Phones

To set Active Directory password:

1. Go to Endpoint > Monitor View.
2. Click Switch Selection Types to select one or more phones to set a unified Active Directory password.
3. Click More > Change Phone Active Directory Password.
4. Enter a new password.
5. Click OK.
   After the operation is completed, click the Download Detailed Report button to view the detailed logs.

Control Call Remotely

You can control a provisioned phone to make a call in the RealPresence Resource Manager system. This feature is supported by Polycom RealPresence Trio and Polycom VVX phones that support REST API.

To control call remotely:

1. Go to Endpoint > Monitor View.
2. Select a supported phone.
3. Click More > Remote Call Control.
4. Enter the destination SIP URI or phone number in the Remote Call dialog.
5. Click OK.

Import Phones Using CSV Files

You can import phones into your RealPresence Resource Manager system via CSV files.

Create a CSV File Containing the Phone Information You Need

You must create a CSV (comma separated values) file that contains the information that you need. You can create this file with any plain text editor or use Microsoft Excel. Do not use Microsoft Excel to edit CSV files on a double-byte operating system.

The RealPresence Resource Manager system define all the imported phones as Polycom Phone by default. When the phones connect to the system, the system will recognize the phone type and model.

| Tips | Limit the phone records number under 10,000 in a CSV file to ensure successful import. |

A CSV file must contain a user defined header to specify the format of phone attributes to be included. Commas (,) are field separators, which cannot be embedded in a field.

Example Header Format (case and sequence insensitive):

```
Phone Model,Phone Type,Serial Number,Phone Location,Phone Status
```

---

Polycom, Inc. 385
mac_address, endpoint_name, owner_id, endpoint_group, reg.1.address, reg.1.displayname, reg.1.auth.userId, reg.1.auth.password, [any attribute name]

Where:

<table>
<thead>
<tr>
<th>Header Attributes</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>• Only mac_address is mandatory.</td>
</tr>
<tr>
<td>endpoint_name</td>
<td>• Do not change the attribute names since they are reserved for the RealPresence Resource Manager.</td>
</tr>
<tr>
<td>owner_id</td>
<td>• The owner_id (local or Enterprise user) format is domain/userid or any owner display name.</td>
</tr>
<tr>
<td>endpoint_group</td>
<td>• Use a pipe (‘</td>
</tr>
<tr>
<td>reg.[1-5].address</td>
<td>• Line information</td>
</tr>
<tr>
<td>reg.[1-5].displayname</td>
<td></td>
</tr>
<tr>
<td>reg.[1-5].auth.userId</td>
<td></td>
</tr>
<tr>
<td>reg.[1-5].auth.password</td>
<td></td>
</tr>
<tr>
<td>attributes</td>
<td>• Refer to the UCS phone attribute names to define attributes.</td>
</tr>
<tr>
<td>Other user defined attributes</td>
<td>• A profile ([MAC_Address]_csv_profile) is automatically generated for each phone that has user defined values.</td>
</tr>
<tr>
<td></td>
<td>• The profile is associated with the phone.</td>
</tr>
<tr>
<td></td>
<td>• Attributes with empty values are ignored in the profile.</td>
</tr>
</tbody>
</table>

**Examples**

Use the following format to add a phone with two line addresses:

`mac_address, endpoint_name, owner_id, endpoint_group, reg.1.address, reg.1.displayname, reg.1.auth.userId, reg.1.auth.password, reg.2.address, reg.2.displayname, reg.2.auth.userId, reg.2.auth.password, 0004F23EA4E1, SoundPoint-EA4E1, ASIAPAC/Jsmith, EP Group 1|EP Group 2, 1000, Jon Smith, 1000, 1000, 1001, Jon Smith1, 1001, 1001`

Use the following format to add a phone with a line address:

`mac_address, reg.1.address 0004F23FD08E, 1001`

Use the following format to add a phone without a line index but an attribute setting in profile:

`mac_address, device.hostname 0004F23EA4E1, SoundPointA4E1 0004F24FD08E, SoundPointD08E`

**Auto Generated Configuration Profile**

If a header in a CSV file contains user defined phone attributes and the attributes for a phone have values, the RealPresence Resource Manager system will generate a configuration profile for this phone.

- The profile name is `Phone_MACAddress_csv_profile`.
- The profile is associated with the phone and has the highest priority by default.
● The profile cannot be associated with other conditions such as Global, Endpoint Group, Site, or Endpoint Models.

● The profile type is CSV Imported. You can filter the CSV imported profiles by profile type on the Endpoint > Phone Management > Configuration Profiles page.

● You can remove this profile from the system. The phone association will also be removed.

Import the CSV File and View the Import Details

You must have either the administrator or area administrator role to import users.

To import phones and view the import details:

1. Go to Endpoint > Monitor View.
3. Click the Choose File button on the Import Audio Phones tab.
4. Browse to the CSV file and select this file.
5. Check the Update the Existing Phone Records check box to update the existing phone in the system.
   Choose one the options:
   ➢ Overwrite Existing Attributes
   ➢ Merge and update. Keep all the phone attributes and update the duplicated attributes.
6. Click the Import button. A Task Progress dialog will show the file uploading and importing progress.
7. View the import details on the Import Phones Result dialog.
8. Download the import log by clicking the Download Import Log button if needed.
9. Click Close to dismiss the Import Phones Result dialog.

Export and Edit Phones

To edit phones' configuration, export the phones' data including the updated attributes in the auto-generated profiles (if any) as a matrix to a CSV file. Then import the CSV file to update phones' data.

Format:
mac_address, endpoint_name, owner_id, endpoint_group, reg.[1-5].address, reg.[1-5].displayname, reg.[1-5].auth.userId, reg.[1-5].auth.password, [any attribute name]

The MAC Address is the unique identifier of a phone. A changed MAC Address is treated as a new phone instead of the updating of the old one.
If a phone's line information is not provisioned by the RealPresence Resource Manager system, the line information will not be exported to the CSV file.

To export manually added phones:

1. Go to Endpoint > Monitor View.
Managing Phones

2 Select More > Import/Export Audio Phones.
3 Click the Export & Download button on the Export Audio Phones tab. The CSV file is downloaded.
4 Open the CSV file and edit the phones’ information if needed.
   For automatically added phones, after the line information is changed, the phones become manually added phones. The mode changes from Auto-added Phones to Manually Added Phones.
   Polycom does not recommend that you change the line information of CUCM synced phones since the changes are overwritten at next CUCM sync interval.

Working with Phone Configuration Profiles

When you manage phones, you can configure them by using configuration profiles. As soon as a phone is configured to use the RealPresence Resource Manager system for its provisioning server, it starts polling for configuration profile updates. The default polling interval is 3:00 am to 5:00 am every day.

To ensure out-of-box usability, the RealPresence Resource Manager system comes with many read-only Polycom standard (pre-defined) configuration profiles. These profiles provide Polycom’s recommended best practice configuration for the associated feature that they enable. You can directly assign these profiles to devices and use them as necessary. Polycom may remove or update Polycom Standard profiles as the configuration recommendation to customers change, or as features are no longer applicable.

Please see the Polycom UC Software Administration Guide for complete documentation on the features of your Polycom phones.

Create a Phone Configuration Profile

You can create new profiles to customize endpoint settings in your environment. You can either create a new one or copy a pre-defined profile and make necessary changes.

Users with the Provision Profiles permission can edit profiles.

To create a configuration profile:

1 Go to Endpoint > Phone Management > Configuration Profiles.
2 Click Add.
3 In the General Information tab of the Add New Configuration Profile dialog, enter a name and description for the new provisioning profile. File name cannot contain / \ : * ? " < > |.
4 Click the Configuration Attributes tab.
5 (Optional) In the Software section, select the endpoint type and a software image.
   The selected version is used to update the phones under certain condition. See Set a Software Update Policy for details.
When a software image is selected, the system will use the attributes defined in its XSD file instead of the default XSD file.

6 Add phone’s provisioning attribute in one of the following ways. When there is an overlap of the attributes, the latest edit will take effect.

- **Standard Fields**
  - Enter text (two or more characters) to search attributes in a XSD file.
  - If you selected a software image with XSD file in the previous step, the system will search attributes in the XSD file packed in the software image.
  - If you have uploaded a customized XSD file from the Endpoint > Phone Management > Phone Management Settings page. The system will search attributes in the uploaded XSD file.
  - The system also comes a default XSD file that contains phone configuration elements that you can use. By default, the system searches attributes in the default XSD file.

- **Custom Fields**
  - You can enter an attribute that is not included in the XSD file and click Apply to add this attribute.
  - XSD validation will not apply to the customized attributes.

- **Import from File**
  - Browse to select a CFG or XML file containing the attributes. The file can contain customized attributes that are not included in the specified XSD file.

- **Paste Configuration XML**
  - Paste a piece of XML containing the attributes and click Apply. You can paste customized attributes that are not included in the specified XSD file.

7 Click OK to save the changes.

**Related Topics**

Set a Software Update Policy

**Edit a Phone Configuration Profile**

You can only edit user defined configuration profiles that you created.

**To edit an customized profile:**

1 Go to Endpoint > Phone Management > Configuration Profiles.
2 Use one of the following ways to open the Edit Configuration Profile dialog.
   - Select a user defined profile and click Edit.
   - Click a user defined profile hyper link. All editable customized profiles are shown as hyper links in blue.
3 As needed, edit the provisioning details.
4 Do one of the following for configuration profiles in use:
Managing Phones

➢ Click **Save and Apply** to apply the updates to the associated on-line phones now. This operation may reboot the phones. If the associated phones are off-line, the phones will receive the changes when the phones connect to the RealPresence Resource Manager system.

If the profile has not been applied to any phones before, **Save and Apply** will not be displayed.

➢ Click **Save** to wait for the updates taking effect automatically at the next polling interval.

If this profile has not been applied to any phones before, click **Save** to save the changes.

For associated phones behind firewall, you can only click **Save** to wait for the updates taking effect automatically at the next polling interval.

**Copy a Configuration Profile**

You can copy a Polycom standard profile or an user defined profile and create your own profiles based on cloned profiles.

To create an customized profile based on a cloned profile:

1. Go to **Endpoint > Phone Management > Configuration Profiles**.
2. Select a profile and click **Clone**.
3. In the **Copy Configuration Profile** dialog, enter a name and description for the new provisioning profile.
4. Edit the attribute as needed.
5. Click **OK**.

**Customize the Configuration Profile List**

You can customize your configuration profile list by using filter.

To customize the Configuration Profile list:

1. Go to **Endpoint > Phone Management > Configuration Profiles**.
2. Click **Filter** to filter configuration profile list by specific conditions.
3. Press **Enter** to do the search.
4. Click **Reset** to clean all the conditions before another search.
5. Enter a key word in the **Search** field beside **Filter** to search the key word among the filter results.
6. Sort the profile list by clicking arrow beside the headings of each column. Special characters such as # and @ cannot be used to sort.

**View CSV Imported Configuration Profiles**

CSV-imported profiles are not displayed by default.
To display CSV imported profiles:
1. Go to Endpoint > Phone Management > Configuration Profiles.
2. Click  .
3. Select CSV Imported as Profile Type.

View a Configuration Profile Detail
You can view the details for both Polycom standard and user defined profiles.

To view details of a profile:
1. Go to Endpoint > Phone Management > Configuration Profiles.
2. Select a profile and click View Details  .
The detail information displays on the right.

Delete a Phone Configuration Profile
You can only delete user defined configuration profiles that you created.

To delete an provisioning profile:
1. Go to Endpoint > Phone Management > Provisioning Profiles.
2. Select an user defined profile and click Delete  .
3. Do one of the following to confirm the deletion:
   - Click Delete and Apply to delete the profile and remove its phones’ association right now.
     This operation may reboot the phones. If the associated phones are offline, the profile association will be removed when the phones connect to the RealPresence Resource Manager system.
     If the profile has not been applied to any phones before, Delete and Apply is not displayed.
   - Click Delete to remove the phones’ profile association. The deletion will apply to the related phones automatically at the next polling interval.
4. If this profile has not been applied to any phones before, click Delete to delete the profile.
   For associated phones behind firewall, you can only click Delete to wait for removing the phones profile association automatically at the next polling interval.

Export Configuration Profiles
This operation export one user defined profile or all user defined profiles to a ZIP file. You cannot export Polycom standard and CSV imported profiles.

To export configuration profile(s):
1. Go to Endpoint > Phone Management> Configuration Profiles.
2. Do one of the following:
Managing Phones

- Select a user defined profile and click Download to export this profile.
- Click More > Export User Defined Profile to export all user defined profiles.

Audio Phone Configuration Profile Deployment

The RealPresence Resource Manager system allows the endpoint admin to use the pre-defined conditions to deploy the configuration profiles for provisioning phones. The following list is ordered by priority of the conditions from the lowest to the highest.

For example, you have a `call.autoAnswer.SIP` parameter enabled in configuration profile A and disabled in configuration profile B. Profile A applies to specific Sites. Profile B applies to Global. The `call.autoAnswer.SIP` parameter is also enabled for all Global phones since Sites has higher priority.

- **Global**: All phones are part of Global regardless of model, site or endpoint group. Configuration profiles association in this container apply to all endpoints.
- **Endpoint Groups**: Configuration profiles association in this container apply to the phones belonging to this Endpoint Group.
- **Endpoint Models/Sites**: Configuration profiles association in this container apply to the phones in a specific endpoint model. For example, apply a customized configuration profile to all Polycom VVX 500 phones.
- **Sites**: Configuration profiles association in this container apply to the phones in a specific site. Geographical locations is the typical use case for site.
- **Endpoints**: Configuration profiles association in this container apply to the phones that you specified. For example, you know specific phones need a specific configuration or call server. You can select these phones to receive the required configuration profiles.

Associate Configuration Profiles with Pre-defined Conditions

You can associate one or more configuration profiles with a pre-defined condition.

To associate profiles to conditions:

1. Go to Endpoint > Phone Management > Profiles Deployment.
2. Associate configuration profiles with one of the following pre-defined conditions:
   - **Global**: Click Edit to open the Edit Configuration Profile Association for Global dialog.
   - **Endpoint Groups/Endpoints**: Select a group or endpoint, click Edit, and click the Configuration Profile Association tab.
   - **Endpoint Models/Sites**: Select a device model or site and click Edit.
     You can search the endpoint model or site by entering a key word in the Search field to search by its name.
3. Select a configuration profile from the Configuration Profile Association drop-down list.
4. Click Apply.
5. Repeat step 3 and step 4 to add more configuration profiles.
6 Adjust the priority of the configuration profiles by clicking the **Arrow** buttons to move the configuration profile up and down or to top or to bottom.

7 Do one of the following:
   > Click **Save and Apply** to apply the updates to the associated on-line phones now. This operation may reboot the phones. If the phones are offline, the phones receive the changes when the phones connect to the RealPresence Resource Manager system.
   > Click **Save** to wait for the updates to take effect automatically at the next polling interval.
   
   For associated phones behind firewall, you can only click **Save** to wait for updates taking effect automatically at the next polling interval.

### Reboot Phones

You can reboot phones for each pre-defined condition.

#### To reboot phones:

1. Go to Endpoint > Phone Management > Profiles Deployment.
2. Reboot phones for one of the following conditions:
   > **Global**: Select More > Reboot All Phones.
   > **Endpoint Groups/Endpoint Models/Sites**: Select a group, device model, or site, select More > Reboot Phones.
3. Click **OK** to confirm the reboot.

### Register Phones to a SIP Server

After registering to a SIP call server, you can make calls using the phones.

#### To register to a SIP sever:

1. Go to Endpoint > Phone Management > Configuration Profiles.
2. Create a profile containing the call server fields.
   
   For example, create a profile named **SIP_server** containing the following fields:
   
   ```
   voIpProt.server.1.address="server_IPaddress"
   voIpProt.server.1.port="Port"
   voIpProt.server.1.transport="TCPpreferred"
   ```
3. Go to Endpoint > Phone Management > Profiles Deployment.
4. Apply the profile to certain phones based on conditions.

### Related Topics

- Create a Phone Configuration Profile
- Associate Configuration Profiles with Pre-defined Conditions
Monitor Phones Behind Firewall

The RealPresence Resource Manager system comes with a pre-defined configuration profile, NotificationServerURL-External. This profile contains the parameters that you need to specify to monitor the SIP register status and call status of phones behind firewall. You can view the status from the Endpoint > Monitor View page.

To monitor phones behind firewall:

1. Go to Endpoint > Phone Management > Configuration Profiles.
2. Click Filter and select Profile Name.
3. Enter NotificationServerURL-External.
4. Click Search.
5. Select NotificationServerURL-External.
6. Click Clone.
7. In the Configuration Attributes tab, replace ProxyServerAddress with your proxy server address in the following parameters. For example, the RealPresence Access Director address.
   - apps.statePolling.URL="https://ProxyServerAddress/PlcmRmWeb/device/PhoneStatus"
   - apps.telNotification.URL="https://ProxyServerAddress/PlcmRmWeb/device/PhoneStatus"
8. Click OK.
9. Go to Endpoint > Phone Management > Profiles Deployment.
10. Apply this profile to the phones behind firewall per the conditions.

Related Topics
View the Endpoint List
Create a Phone Configuration Profile
Associate Configuration Profiles with Pre-defined Conditions

Working with Resource Files

Resource files can be any type of file used for configuring phones. For example, you can upload image files and configure the system to use the files as phone icons in your configuration profile.

When you upload a global 000000000000-* file, for example, 000000000000-directory.xml, or 000000000000-license.cfg file, this file will be applied to all the phones that are provisioned by the RealPresence Resource Manager system. phones will read the parameters in the 000000000000-* file after connecting to the system. See Polycom UC Software Administrator Guide for details on phone configuration files.

Upload Resource File

Uploading resource files under 50 MB is recommended.
To upload resource file:
1. Go to Endpoint > Phone Management > Resource Files.
2. Click Add to open the Upload Resource Files dialog.
3. Browse to the file to be uploaded.
4. Enter a description.
5. Click OK to upload the file.

**Download Resource File**
You can download the resource files and check the content.

To download resource file:
1. Go to Endpoint > Phone Management > Resource Files.
2. Select a resource file to download. You can download a single file each time.
3. Click Download to download the selected file.

**Delete Resource Files**
You can delete one or more resource files.

To delete resource files:
1. Go to Endpoint > Phone Management > Resource Files.
2. Select a resource file or click Switch Selection Types to select multiple resource files.
3. Click Delete.
4. Click OK to confirm the deletion.

**Refresh Resource Files**
Refresh the Resource Files page to see the resource files changes made by other users.

To Refresh resource files:
1. Go to Endpoint > Phone Management > Resource Files.
2. Click Refresh.

**Customize the Resource File List**
You can customize your resource file list by using filter.
To customize the Endpoint Group list:

1. Go to Endpoint > Phone Management > Resource Files.
2. Click Filter to filter resource files by File Name or Uploaded By condition.
3. Press Enter to do the search.
4. Click Reset to clean all the conditions before another search.
5. Enter a key word in the Search field beside Filter to search the key word among the filter results.

Setting up Phone Software Updates

You can update the software on your provisioned phones automatically with the RealPresence Resource Manager system.

Upload the Software Update for Phone Software Updates

Polycom recommends you to do software updates using the split packages available on Polycom’s support website to reduce system resource consuming.

When a large number of phones applies for updates at the same time, the updates may not be completed at one time.

To upload a software update:

1. Go to Endpoint > Phone Management > Upload Software Updates.
2. Click Add to open the Upload Software Update dialog.
3. In the Software Update File section, do one of the following:
   - Click Choose File to browse to the software update file you downloaded.
   - Select the Polycom Hosted Server radio button and select a phone type that you want to update.
     The system will search the available software images on the specified Polycom server. All the available phone images will show in the Software Available drop-down list. Select a version that you want to upgrade to.
4. Enter a meaningful description that will help other users to understand the purpose of the software update.
5. In the Attach to Configuration Profile section, select one of the following options:
   - Do not attach to a configuration profile: do not associate this software update with any configuration profile.

Web proxy server is not supported for connecting Polycom Hosted Server. You need to configure the access from the RealPresence Resource Manager system.
Managing Phones

- Create a new configuration profile base on software version: create a new configuration profile and associate this software update with the profile.
- Attach to existing configuration profile: select an existing profile from the drop-down list and associate the software update with the profile.

After the software update is associated with a profile, you can open the new or existing profile from the Endpoint > Phone Management > Configuration Profiles page, the software update is selected in the Software field for this profile.

6 Click OK to upload the software image.

You will see the download progress in the Download Phone Software dialog. You can close this dialog, the download still continues. After the download is done, you will see the downloaded phone software image from the Endpoint > Phone Management > Upload Software Updates page.

**Customize Software Updates List**

You can customize your software update list by using filter.

To customize the Endpoint Group list:

1. Go to Endpoint > Phone Management > Upload Software Updates.
2. Enter a key word in the Search field to search by File Name, Description, and Uploaded By.

**Enable System Alerts for New Software Updates on Polycom Hosted Server**

After enabling the system alerts, when new phone software updates are available on the Polycom Hosted Server, the RealPresence Resource Manager system will detect the updates and raise alerts for the changes.

Web proxy server is not supported for connecting Polycom Hosted Server. You need to configure the access from the RealPresence Resource Manager system.

To enable system alerts for new software updates on Polycom Hosted Server:

1. Go to the Endpoint > Phone Management > Upload Software Updates page.
2. Click MORE > Enable System Alerts for Endpoint Software Updates.
3. Check the Enable system alerts for updates on the Polycom Hosted Server for the following endpoints: check box.
4. Select the endpoint types that you want to watch.
5. Click OK.
Set a Software Update Policy

After uploading software updates, you can create or use existing configuration profiles for the phone updates, set update versions in the configuration profiles, and apply the profiles to different phones under certain conditions.

For CX5X00 updates, the update interval (device.local.updateInterval) must be longer than 604800 seconds, otherwise the update time (device.local.updateTime) will not take effect. See the UCS phone documentation for details on parameter settings.

To set software update versions:

1. Go to Endpoint > Phone Management > Configuration Profile.
2. Select a specific profile that you want to use to do phone updates.
3. In Configuration Attributes, select a software version to use.
4. Go to Endpoint > Phone Management > Profile Deployment.
5. Deploy this the configuration profile to a condition that you want.
6. Do one of the following:
   - Click Save and Apply to upgrade the associated on-line phones now.
   - Click Save to save the changes. The next time the phones under this condition poll the RealPresence Resource Manager system, the phones will detect the new software version, so the phones will automatically download and install the identified software update package. Use this method to force users to use a specific software version.

Managing RealPresence Group Series Via Polycom Trio

You can manage and update a RealPresence Group Series system via a Polycom Trio system when they pair.

The RealPresence Resource Manager system can provision the specific RealPresence Group Series parameters that Polycom Trio supports. You also can update a paired RealPresence Group Series system by creating a configuration profile to set the download URL and upload its software update file.

If you want to upgrade both RealPresence Group Series and Polycom Trio when they pair, both systems require a configuration profile. Therefore, you need one configuration profile that specifies Group Series as the endpoint type, and another one that specifies an endpoint type as Polycom Phone.

Related Topics

Working with Phone Configuration Profiles
**Upload the Software Update for RealPresence Group Series Endpoints**

Polycom recommends you to do software updates using the split packages available on Polycom Support to reduce consuming system resources.

The RealPresence Resource Manager system doesn’t generate a configuration profile automatically after you upload a RealPresence Group Series image.

To upload the software package and create a software update:

1. Go to Endpoint > Phone Management > Upload Software Updates.
2. Select Group Series from the Endpoint Type drop down list.
3. Click Add.
4. If an activation key code is required to activate the software update:
   a. Select the Update Requires Key check box.
   b. In the Software Update Key File field, browse to the .txt key file you received in Request Upgrade Activation Keys.

   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.

   After uploading a software image, you cannot view the key file anymore. To update the file, you must re-upload the software with updated key file.

5. In the Software Update File field, browse to the software update file you downloaded.
6. Enter a meaningful description that helps other users to understand the purpose of the software update.
7. Click OK.

   A software image for RealPresence Group Series endpoints is created. You can view the software image at Endpoint > Dynamic Management > Upload Software Updates and at Endpoint > Phone Management > Upload Software Updates when you choose Group Series as the endpoint type.

**Related Topics**

Request Upgrade Activation Keys

**Working with CUCM**

When you integrate a Cisco Unified Communications Manager system with your RealPresence Resource Manager system, the RealPresence Resource Manager system becomes aware of all of the supported Polycom phones registered to the Cisco Unified Communications Manager. Supported phones are
displayed in the **Endpoint > Monitor View** page, and the RealPresence Resource Manager system can use information about these phones to deliver provisioning information.

- Polycom highly recommends you to re-integrate CUCM after upgrading to 10.1.
- After upgrading to 10.1, you must manually update the phones’ provisioning protocol to HTTP or HTTPS and specify the RealPresence Resource Manager system IP address. See [Configure Automatically Added Phones for Provisioning](#) for details.

Setting up a CUCM server to work with the RealPresence Resource Manager system includes the following tasks:

- Configuring Cisco Unified Communications Manager
- Enabling Auto Discovery of RealPresence Resource Manager through DHCP
- Creating Phone Configuration Profiles
- Customizing Digest User Password
- Integrating with a Cisco Unified Communications Manager

### Configuring Cisco Unified Communications Manager

The RealPresence Resource Manager system uses Cisco AXL SOAP API to enable integration with the Cisco Unified Communications Manager. This web service is disabled by default. You’ll need to enable it, and create a user with the appropriate privileges to use with the RealPresence Resource Manager system.

### Start the Cisco AXL Web Service

In your Cisco Unified Communications Manager system, you’ll need to activate the Cisco AXL Web Service before you create a new user.

**To activate the service:**

1. From the **Unified CM Administration** window, go to **Navigation > Unified CM Serviceability**.
2. Choose **Tools > Service Activation**.
3. From the **Server** box, choose the server and click **Go**.
4. From the **Database and Admin Services** section, select **Cisco AXL Web Service** and save the changes.

### Creating a User for the RealPresence Resource Manager Integration

In your Cisco Unified Communications Manager, you need to create an Access Control Group with the correct role and then add your newly-created user to that group.

By default, the administrator has the correct privileges for integration. Although not recommended, you can use this user for an initial test or quick set up.
Create the Access Control Group

In the Cisco Unified Communications Manager system, Access Control Groups are used to organize users and their roles.

To create an Access Control Group with AXL API role:

1. In the Cisco Unified Communications Manager system, ensure that the Standard AXL API Access role exists. Choose User Management > User Settings > Role.
3. Click Add New.
4. In the Access Control Group Information dialog box, name your access control group. For example, Polycom RPRM Integration.
5. Click Save to save the name.

Assign AXL role to the Group

In the Cisco Unified Communications Manager system, you'll need to assign the Standard AXL API Access role to the new group.

To assign the role:

2. Click Find to list all the groups.
3. Select the group you created and click Assign Role to Group, and select Standard AXL API Access to assign it to the new group.
4. Click Save.

Create the User

In the Cisco Unified Communications Manager, you should create a new user to use for integration with the RealPresence Resource Manager system.

To create a new user:

2. In the Add New User dialog, enter a name for your new user. For example, rprmint.
3. Click Add to Access Control Group to add the access control group you created.
4. Click Save to save the user information.

After completing each of these sections, your Cisco Unified Communications Manager is ready to be integrated with the RealPresence Resource Manager system.
Enabling Auto Discovery of RealPresence Resource Manager through DHCP

The phones will use the DHCP option 66 to discover the RealPresence Resource Manager system. See Polycom UC Software Administrators’ Guide for detailed information.

Creating Phone Configuration Profiles

You should create your phone provisioning profiles before integrating your system with a Cisco Unified Communications Manager. Phones registered with the Cisco Unified Communications Manager begin polling for provisioning updates via HTTP or HTTPS after you integrate your Cisco Unified Communications Manager with your RealPresence Resource Manager system. After initial provisioning, provisioning updates are sent according to the provisioning poll you configure.

Configuring the CUCM as a SIP server (Optional)

If you want to use the CUCM server, you need to configure the SIP registration server to the CUCM in a profile.

Related Topics

Register Phones to a SIP Server

Customizing Digest User Password

Optionally, you can customize the digest user password for the phones you provision. When you integrate with a Cisco Unified Communications Manager system, each phone’s password is reset to the factory default. By default, a system-generated password is used. You can change this password at any time.

Related Topics

Configure Your Phone Management Settings

Integrating with a Cisco Unified Communications Manager

You can integrate only one CUCM server with the RealPresence Resource Manager system to synchronize the phones from the CUCM server.

Add a Cisco Unified Communications Manager

You can add a Cisco Unified Communications Manager system to your RealPresence Resource Manager system. The RealPresence Resource Manager begins provisioning phones as soon as you add the Cisco Communications Manager system to your RealPresence Resource Manager system.
To add a Cisco Unified Communications Manager for provisioning:

1. Go to Network Device > Instances.
2. Click Add .
3. In the Add Instance dialog box, select Cisco Unified Communications Manager from the Device Type drop-down list. Complete settings.
4. Click OK.

The system integrates with the Cisco Unified Communications Manager and begins provisioning phones.

Adding Cisco Unified Communications Manager Settings

The table explains the

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>You can only add a Cisco Unified Communications Manager system by IP or FQDN address.</td>
</tr>
<tr>
<td>Add By</td>
<td>The name of the Cisco Unified Communications Manager system.</td>
</tr>
<tr>
<td>Device Name</td>
<td>The IP address of the Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Management Address</td>
<td>Enter the user name used to connect with the Cisco Unified Communications Manager. This user must have the AXL API Access Role. See Working with Phone Configuration Profiles.</td>
</tr>
<tr>
<td>Admin Password</td>
<td>Enter the user name password.</td>
</tr>
<tr>
<td>Service Integration</td>
<td>Select the check box if the Cisco Unified Communications Manager is integrated with the same Active Directory as the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>CUCM is Integrated with same AD as Resource Manager</td>
<td>If you marked the CUCM is Integrated with the same AD as Resource Manager check box, please enter the user ID that the Cisco Unified Communications Manager system used to integrate with the Active Directory.</td>
</tr>
<tr>
<td>LDAP Attribute for CUCM User ID</td>
<td>Configure how often you want the RealPresence Resource Manager to synchronize with the Cisco Unified Communications Manager to retrieve the list of registered Polycom phones. If you are using Cisco Unified Communications Manager v10 or higher, Polycom recommends synchronizing every five to seven days.</td>
</tr>
</tbody>
</table>

Synchronize with the Cisco Unified Communication Manager

When you synchronize your system with the Cisco Unified Communications Manager, the RealPresence Resource Manager system retrieves information about any added phones since the last time you
synchronized. Synchronization happens automatically when you first integrate with a Cisco Unified Communications Manager.

If you are using Cisco Unified Communications Manager 10 or higher, all added Polycom phones are automatically synchronized to the RealPresence Resource Manager every 10 minutes.

You can choose to synchronize with the Cisco Unified Communications Manager at any time.

To synchronize with a Cisco Unified Communications Manager:

1. Go to Network Device > Instances.
2. Select the Cisco Unified Communications Manager you want to synchronize.
4. Click Close after the synchronization is done.

Configure Your Phone Management Settings

You can configure the following phone settings from the Endpoint > Phone Management > Phone Management Settings page:

- **Digest Password for CUCM Synced Phones**: After you integrate with a Cisco Unified Communications Manager, the digest password for the phones is reset to the factory default unless you change this password. You can also customize the digest user passwords for the phones.

- **Provisioning Account Configuration**: The HTTP or HTTPS service is used for the provisioning connection between the RealPresence Resource Manager system and the phones. By default, a system-generated user name and password are used by the phones during the process to get provisioning profiles and software updates from the RealPresence Resource Manager. Each phone uses the same HTTP or HTTPS service password. The default user name and password are both PlcmSpIp.

   You can change this password at any time. After you change the password, you need to configure the phones to use the same HTTP or HTTPS password. Otherwise, the phones will not be able to connect to the RealPresence Resource Manager system to receive provisioning profiles and software updates.

   If phone communicates with RealPresence Resource Manager via HTTPS, you should ensure that the phone(s) can validate the RealPresence Resource Manager system’s security certificate. For more information about certificates RealPresence Resource Manager system certificates, see Security Certificates. For information about certificates for Polycom phones, see the respective UC Software Administrator Guide.

- **Phone Files Rotation Settings**: You can control the disk space that the uploaded configuration and log files occupy in the RealPresence Resource Manager system. The default values rotate the log files every 1024 KB and keep up to five files for 15 days.

   The logs are saved in the /var disk. When the /var disk 90% occupied, the system will clean the logs automatically. For example, if the Days to Retain Phone Files value is 15 days, when the /var disk 90% occupied, the system will clean the logs saved on the first day. If the /var disk still 80% occupied, the system will keep cleaning the logs saved on the second day.
To configure phone management settings:

1. Go to **Endpoint > Phone Management > Phone Management Settings**.
2. To change the digest password for phones synced from Cisco Unified Communications Manager:
   a. In the **Digest Password for CUCM Synced Phones** section, clear the **Use System Auto Generated Password** check box.
   b. Complete **Password** and **Confirm Password** fields.
3. In the **Maximum Disk Space for Resource Files** section, enter a maximum size and click **Update**. The supported range of the maximum size is: 50MB - 250MB
4. In the **Phone Files Rotation Settings** section, change the settings as needed and click **Update**. The range of the settings is:
   - **Log File Rotation Size**: 512KB - 10240KB
   - **Number of Retaining Files (per name)**: 1 - 10
   - **Days to Retain Phone Files**: 0 - 30
5. To configure the provisioning account, in the **Provisioning Account Configuration** section, edit the **User Name** or the **Password**.
6. To upload a XSD file, in the **Upload Default XSD** section, browse to the XSD file and click the **Upload** button.
7. Click **Update**.
User Management

The RealPresence Resource Manager system uses roles to define permissions. Users can be assigned management roles, associated with endpoints, and organized in groups.

You can assign roles and provisioning profiles to sets of users by using 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.
Working with Users

The RealPresence Resource Manager system supports two types of users.

- Users that are local to the management system. These users are added manually to the system or imported from a file.
- Enterprise users that come directly from the enterprise directory.

If your company has implemented multi-tenancy, you can also assign local users or enterprise users to an area or areas that you manage.

Related Topics
Configuring Multi-Tenancy

Local Users

After you manually add local users (or import them), 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 can dial into conferences. However, the system cannot dial out to them until they are associated with endpoints.

You can associate local users with one or more roles as well as one or more endpoints. Alternatively, you can associate local users with local groups and then assign roles to an entire group.

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 email address, system password, and so on.
Users imported into the system through the enterprise directory are added to the system without a role. This default setup enables 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.

Managing Local Users

Users assigned the Administrator role can add, import, update, or delete local users.

Add a Local User

You can add local users.

You need to have the administrator role to add a local user.

To add a local user:

1. Go to User > Users and click Add. The Add New User dialog appears. The User Enabled option is selected by default.
2. Enter the user information.
3. If needed, click the Create Password button to generate a random password by the system.
4. Click Save.
5. 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. If the user has multiple endpoints, list the endpoints in order of priority, with the primary endpoint first. 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.
6. 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.
7. 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.

8 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.

9 In the Associated Alert Profile section, select a Remote Alert Notification Profile as appropriate.

10 In the SIP Dial String Reservations section, select the user’s Endpoint Type and enter the appropriate dial string for SIP URI, then click Apply.

The dial strings appear in the list below.

By default, the same SIP URI is used for all endpoints that belong to the same user. If the user has multiple endpoints and you want a different SIP URI for each endpoint type, enter the dial strings for one endpoint type at a time and click Apply each time.

11 In the H323 Dial String Reservations section, select the user’s Endpoint Type and enter the appropriate dial string for 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.

12 Click Update.

If the Phone Number you entered is exactly the same as an existing user or endpoint, the Phone Number Conflict dialog 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.

User Information

Enter the 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>
<tr>
<td>User ID</td>
<td>The user’s unique login name. This user ID must be unique across all rooms and users and across all domains. For Multi-Tenancy: 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 <a href="mailto:bsmith@tenantA.com">bsmith@tenantA.com</a> as a user name and Bob Smith in TenantB could have <a href="mailto:bsmith@tenantB.com">bsmith@tenantB.com</a>.</td>
</tr>
</tbody>
</table>
Import Local Users

You can import local 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.

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.

You need to have either the administrator or area administrator role to import users.

To import local users:

1. Create a CSV file that contains the user information.
2. Choose User > Users and click Import Local Users from the More drop-down list.
3. In the File Location (CSV) field, browse to the location of the CSV file you created.
4. If areas are enabled and you manage more than one area, select an area from the Assign Area drop-down list.
   - 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 the 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.
5. Click Import.
   - A status window appears. Click OK when it is complete.
   - 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.
9 Review the import details file that you downloaded.

**Sample CSV file of User Information**

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.

Only UTF-8 encoding is supported in the CSV file.

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.
- 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>
</tbody>
</table>
Working with Users

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, ,

Troubleshooting 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. 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.

Handle the User Accounts with Password Lost

If you fail to record or remember the password shown on the Import Summary screen, there will be no other way to determine the password 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 system generate a password.

Delete all affected users one-by-one via the RealPresence Resource Manager user interface and re-import them.

Updating Local 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),

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<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>
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 RealPresence 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 RealPresence 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.

Delete a Local User

You can only delete local users from the RealPresence Resource Manager system. You cannot delete users added through integration with an enterprise directory.

You need the Administrator role to delete users.

To delete a user:

1. Go to User > Users.
2. Search the user you want to delete.
3. Select the user and click Delete.
   - To delete multiple users, hold the Shift key down while you make your selections.
4. Click OK to confirm the deletion.
   - The user is deleted from the system.
**Managing Users**

Users assigned the **Administrator** role can manage both local users and enterprise users.

**Search for a User**

You can search for a user. Searches for a user are case-insensitive, prefix searches of the User ID, First Name, and Last Name fields.

You must log in as an enterprise user to search for enterprise users.

**To search for a user:**

1. Go to **User > Users**.
2. In the Search Users field, enter the following keywords to search the users of interest.
   - **First Name** The first name of the user of interest.
   - **Last Name** The last name of the user of interest.
   - **User ID** The user ID of the user of interest.
   - **Domain** Enter **Local** to search for local users. Enter a domain name to search for enterprise users.
3. Press **Enter**.

The first 500 users in the database that match your search criteria are displayed in the **Users** list. 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 a user information:**

1. Go to **User > Users**.
2. Select the user you want.
3. Click **Edit** to view the user information.

**User Information Details**

The table lists the user information details.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td></td>
</tr>
<tr>
<td><strong>First Name</strong></td>
<td>The user’s first name</td>
</tr>
</tbody>
</table>
Working with Users

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.

You need the Administrator role to edit users.

To edit a user:

1. Go to User > Users.
2. Search for the user you want to edit.
3. Select the user you want to edit and click Edit

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 and users and across all domains.</td>
</tr>
<tr>
<td>Email Address</td>
<td>The user’s email address. (The Email address is an ASCII-only field.)</td>
</tr>
<tr>
<td>Title</td>
<td>The user’s professional title.</td>
</tr>
<tr>
<td>Department</td>
<td>The user’s department within the enterprise.</td>
</tr>
<tr>
<td>City</td>
<td>The city in which the user’s office is located.</td>
</tr>
<tr>
<td>Contact Number</td>
<td>The contact phone number for the user.</td>
</tr>
<tr>
<td>Assign 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>
<tr>
<td>Belongs to Area</td>
<td>This field is only available if Areas have been enabled.</td>
</tr>
<tr>
<td>Manages Area</td>
<td>This field is only available if Areas have been enabled.</td>
</tr>
<tr>
<td>Create Password</td>
<td>Click the Create Password button to generate a password by the system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Associated Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned Roles</td>
<td>The roles assigned to the user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Groups</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of group to which the user belongs. Possible values are local and enterprise.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the group to which the user belongs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inherited Group Info</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book</td>
<td>The Address Book(s) the user sees based upon the groups to which the user is assigned.</td>
</tr>
</tbody>
</table>
4 As required, edit the General Info, Associated Endpoints, Associated Roles, Managed Areas, Associated Alert Profile, and Dial String Reservations sections of the Edit User dialog.

If the user has multiple associated endpoints, list the endpoints in order of priority, with the primary endpoint first.

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.

5 Click Update.

Assign Users to Manage an Area(s)

You need the Administrator role to enable areas (multi-tenancy) and assign users to manage an area.

In order to perform RealPresence Resource Manager system 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 Search for the user you want to assign to an area.

3 Select the user and click Edit.

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 In the Available Areas section, select 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 select area(s) in the Selected Areas section and click the corresponding arrow to move the selected area(s) to the Available Areas section.

The user will be assigned to manage the areas in the Selected Areas section.
Enable/Disable Users

Be default, a user is enabled to use the system when you create the user. However, after some period of inactivity users may become disabled.

You can enable or disable multiple users at once.

You need the Administrator role to enable or disable users.

To enable or disable multiple users:

1. Go to User > Users
2. Select the user you want to enable or disable and click Edit.
3. Check or clear User Enabled.
   The users are enabled or disabled.

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.

You need the Administrator role to enable or disable users.

To unlock a user account:

1. Go to User > Users and search for the user you want to unlock.
2. Select the user whose account you want to unlock and click Edit.
3. Clear the User Locked check box.
4. Click Update.
5. The system should allow the user to log in.

Clear Orphan Active Directory Users/Rooms

When a user or room is deleted from your Active Directory system, it is not automatically deleted from your RealPresence Resource Manager system. You may want to periodically update your user list when you are integrated with an Active Directory system.

Use the Clear Orphan Active Directory Users/Rooms option to delete enterprise users that are listed in your system, but no longer exist in Active Directory.

You need the Administrator role to clear the orphan Active Directory users or rooms.

Be sure your Active Directory Connection is Available.
If you perform an orphan clean up when your system is not connected to Active Directory, you will delete ALL users in the system.
To delete orphaned Active Directory users:

1. Go to User > Users.
2. Select Clear Orphan AD User/Roo ms from the More drop-down list.
3. Click OK.

All enterprise users that no longer exist in your enterprise directory are deleted from your RealPresence Resource Manager system.

Managing Dial String Reservations for Users

If you need to make multiple dial string reservations for multiple users, you can use the Import User Alias function. If you need to make a report of which dial strings (H.323 or SIP URIs) have been reserved for each user, you can use the Export User Alias function.

Both the Import User Alias and Export User Alias features allow you to manage the dial string reservations for all users at once. If you need to only add or modify a dial string for a single user, it is more efficient to edit that user’s dial strings directly.

Dial string reservations take first priority when they are associated with a user and will overwrite any provisioned H.323 alias or SIP URI for that user.

Specifically, SIP URI dial string reservations are assigned in the following three ways, listed by priority:

1. Dial string reservation associated with user record.
2. Domain user or third-party server (for example, Microsoft Lync).
3. Auto-generated SIP URI through the RealPresence Resource Manager system.

Export User Aliases

You can export a report of users with reserved SIP URI aliases, either SIP or H.323. Keep in mind that this CSV file will contain displays reserved aliases and dynamically provisioned aliases if the provisioning information has already been sent.

Users with the area administrator role can only export aliases from one area at a time or from only the areas they manage. Users with the administrator role can export alias information from all areas.

To export a list of user aliases:

1. Navigate to User > Users.
2. Click Export User Aliases from the More drop-down list.
3. In the Export User Aliases dialog, select the SIP radio button and click Export.
   - You cannot export both H.323 and SIP aliases in the same report. You must export them separately.
4. Save the report.
Importing User Aliases

You can import a list of user aliases that will add to or overwrite any existing reserved dial string aliases that have been associated with users.

You will need to create a CSV (comma separated values) file that lists the user information and user alias reservations you wish to add or update. You may use any text editor or Microsoft Excel to create the CSV file.

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.
- 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.

SIP Format:

Domain, username, endpoint type, SIP URI, Endpoint Name

Where:

Commas (',') are used as field separators and cannot be embedded in a field. The endpoint name should be used if you need to differentiate between two endpoint names (HDX1 and HDX1) of the same endpoint type for the same user. The endpoint name is required in order to associate the SIP URI with a device. You do not need to include a SIP URI for all users in the file, but at least one user must have a value for the SIP URI field.

The following fields are required: **Domain, Username, Endpoint Type**, and **SIP URI**. Other fields can be left blank, but not skipped.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Specifies the domain of the user.</td>
</tr>
<tr>
<td>Username</td>
<td>The username must already exist in the RealPresence Resource Manager system. This can be the user ID of a user or a machine account, or the name of a room.</td>
</tr>
</tbody>
</table>
### Examples

- This first example reserves the SIP URI to all endpoint types for this user:
  ```
  local, johndoe, All_Types, johndoe@example.com
  ```
- This example reserves the SIP URI to the HDX for this user.
  ```
  local, johndoe, HDX, johndoeHDX@example.com
  ```
- This example reserves the SIP URI to the HDX that is named johndoeHDX2.
  ```
  local, johndoe, HDX, johndoeHDX2@example.com, johndoeHDX2
  ```

### H323 Format

**Domain, Username, Endpoint Type, H.323 ID, E.164 Number, Endpoint Name**

**Where:**

Commas (','), are used as field separators and cannot be embedded in a field. The endpoint name should be used if you need to differentiate between two endpoint types (HDX1 and HDX1) of the same type for the same user. You can supply an H.323 ID, an E.164 number or both. You do not need to enter a dial string for each user in the file.

The following fields are required: **Domain, Username, Endpoint Type, H323 ID and E.164**. Other fields can be left blank, but not skipped.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint Type</strong></td>
<td>The following are valid endpoint types:</td>
</tr>
<tr>
<td></td>
<td>HDX</td>
</tr>
<tr>
<td></td>
<td>VVX</td>
</tr>
<tr>
<td></td>
<td>CMADesktop</td>
</tr>
<tr>
<td></td>
<td>RPMobile</td>
</tr>
<tr>
<td></td>
<td>GroupSeries</td>
</tr>
<tr>
<td></td>
<td>RPDesktop</td>
</tr>
<tr>
<td></td>
<td>ITP</td>
</tr>
<tr>
<td></td>
<td>RPDebut</td>
</tr>
<tr>
<td></td>
<td>RPCentro</td>
</tr>
<tr>
<td></td>
<td>CX</td>
</tr>
<tr>
<td></td>
<td><strong>All_TYPES</strong></td>
</tr>
<tr>
<td><strong>URI</strong></td>
<td>The SIP URI for this user. The SIP URI supports alphanumeric characters and the following special characters: '.', '-', '_', '@', ':'.</td>
</tr>
<tr>
<td><strong>Endpoint Name</strong></td>
<td>The endpoint name should be included if you need to differentiate between two endpoint names (jsmithHDX1 and jsmithHDX2) for the same endpoint type for the same user.</td>
</tr>
</tbody>
</table>
Working with Users

Examples

- This first example reserves the H.323 ID and E.164 number for this user’s HDX system.
  `local,johndoe,HDX,johndoeHDX,771000`
- This example updates the H.323 ID and E.164 number for this user’s “johndoeHDX2”.
  `local,johndoe,HDX,johndoeHDX2,771001`

Importing User Aliases

You can import user aliases.

To import a list of user aliases:

1. Create a valid CSV file to use. It may be helpful to use an exported User Alias CSV file on which to base your changes.
2. Navigate to User > Users.
3. Select Import User Aliases from the More drop-down list.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Specifies the domain of the user.</td>
</tr>
<tr>
<td>Username</td>
<td>The username must already exist in the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td></td>
<td>This can be the user ID of a user or a machine account, or the name of a room.</td>
</tr>
<tr>
<td>Endpoint Type</td>
<td>The following are valid endpoint types:</td>
</tr>
<tr>
<td></td>
<td>HDX</td>
</tr>
<tr>
<td></td>
<td>VVX</td>
</tr>
<tr>
<td></td>
<td>CMADesktop</td>
</tr>
<tr>
<td></td>
<td>RPMobile</td>
</tr>
<tr>
<td></td>
<td>GroupSeries</td>
</tr>
<tr>
<td></td>
<td>RPDesktop</td>
</tr>
<tr>
<td></td>
<td>ITP</td>
</tr>
<tr>
<td></td>
<td>RPDebut</td>
</tr>
<tr>
<td></td>
<td>RPCentro</td>
</tr>
<tr>
<td></td>
<td>CX</td>
</tr>
<tr>
<td></td>
<td>All_Types</td>
</tr>
<tr>
<td>H.323 ID</td>
<td>The H.323 ID for this user. The H.323 ID supports alphanumeric characters and the following special characters: '.', '-', '_', '@', ':'.</td>
</tr>
<tr>
<td>E.164 Number</td>
<td>The E.164 number for this user. The E.164 number must consist of only numeric characters.</td>
</tr>
<tr>
<td>Endpoint Name</td>
<td>The endpoint name should be included if you need to differentiate between two endpoint names (jsmithHDX1 and jsmithHDX2) for the same endpoint type for the same user. The endpoint name is required if you want to associate the SIP URI with a particular endpoint name that has been assigned to a user.</td>
</tr>
</tbody>
</table>
4 In the **Import User Aliases** dialog, select **SIP** aliases or **H323** aliases radio button and click **Export**. You cannot import both H.323 and SIP aliases in the same report. You must export them separately.

5 Click **Update**.

An error message will display if your CSV file contained any mistakes. If you get an error message, you will need to correct the rows that were not loaded and import them again.
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.

Conference 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.

Understanding User Roles

The RealPresence Resource Manager system is a role and permissions based system.

- Users can be 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 related—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 you have 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.

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.
   
   To ensure system access and stability, the default administrator role cannot be deleted or edited.

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 multiple roles. 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 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.

Managing User Roles

You can assign roles to both local and enterprise users.

Only users assigned the Administrator role can manage user roles.

View the List of User Roles

You can view a list of the user roles for your system.

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. The Name is the unique name of the user role.

Add a User Role

When you add a user role, you also specify permissions for the role.

You need the Administrator role to add a user 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 and assign permissions to the new role.
4. Click Update.

The new user role appears in the RealPresence Resource Manager system.

Adding Role Settings

The following table describes the fields of the Add Role dialog.
Working with Management Roles and Permissions

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.

- Do not edit pre-defined roles for system that needs high security.

You need the Administrator role to add a user role.

To edit the permissions for a user role:

1. Go to User > User Roles.
2. As needed, click Filter to customize the User Roles list.
3. In the User Roles list, select the role you want to edit and click Edit.
4. Edit the Description field of the Edit Role dialog and edit permissions for the role.
5. Click Update.

Delete a User Role

You can delete a user role from the RealPresence Resource Manager system, provided no users are currently assigned to it.

You need the Administrator role to add a user role.

<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 Permissions</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>
</tbody>
</table>
To delete a user role:

1. Go to User > User Roles.
2. As needed, use Filter to customize the User Roles list.
3. In the User Roles list, select the role you want to delete 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

You can view the users and groups that have been associated with a role.

To view which groups and users are associated with a specific user role:

1. Go to User > User Roles.
2. As needed, use Filter to customize the User Roles list.
3. In the User Roles list, select the role you want to view and click View Associated Groups and Users from the More drop-down list.

The View Associated Groups and Users dialog appears.

Assigning Roles to Enterprise Users

If you want the RealPresence Resource Manager system to, by default, automatically assign enterprise users the basic Scheduler role, you must change the appropriate system Security Settings.

You need the Administrator role to add a user role.

Enabling and Editing Log in Banners

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 provides administrators almost unlimited flexibility in defining roles, for simplicity and clarity, Polycom recommends keeping the default roles with their default permissions and responsibilities. Because users can be assigned multiple roles, and permissions are cumulative, you can combine roles as needed to reflect the workload your people undertake to manage and use the system.
<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler</td>
<td>Schedule Conferences&lt;br&gt;Scheduling Level = Basic&lt;br&gt;&lt;br&gt;&lt;strong&gt;When areas are enabled:&lt;/strong&gt;&lt;br&gt;View and/or modify all areas. Can perform role tasks in all areas.</td>
</tr>
<tr>
<td>Advanced Scheduler</td>
<td>Schedule Conferences&lt;br&gt;Scheduling Level = Advanced&lt;br&gt;&lt;br&gt;&lt;strong&gt;When areas are enabled:&lt;/strong&gt;&lt;br&gt;View and/or modify all areas. Can perform role tasks in all areas.</td>
</tr>
<tr>
<td>View-Only Scheduler</td>
<td>Schedule Conferences&lt;br&gt;Scheduling Level = View-Only&lt;br&gt;&lt;br&gt;&lt;strong&gt;When areas are enabled:&lt;/strong&gt;&lt;br&gt;View and/or modify all areas. Can perform role tasks in all areas.</td>
</tr>
<tr>
<td>Operator</td>
<td>Conference Operator&lt;br&gt;Report Operator&lt;br&gt;Troubleshooting&lt;br&gt;Schedule Conferences&lt;br&gt;Scheduling Level = Advanced&lt;br&gt;&lt;br&gt;&lt;strong&gt;When areas are enabled:&lt;/strong&gt;&lt;br&gt;View and/or modify all areas. Can perform role tasks in all areas.</td>
</tr>
<tr>
<td>Device Administrator</td>
<td>Add endpoints and network devices.&lt;br&gt;Network Device Admin&lt;br&gt;Assign Provisioning Profiles through scheduled management&lt;br&gt;Schedule software updates for endpoints&lt;br&gt;&lt;br&gt;&lt;strong&gt;When areas are enabled:&lt;/strong&gt;&lt;br&gt;View and/or modify all areas. Place devices and endpoints in Areas</td>
</tr>
</tbody>
</table>
## Scheduler Roles, Responsibilities, and Menus

The RealPresence Resource Manager system offers three different default Scheduler roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
</table>
| Administrator       | Directory Setup  
This role cannot be deleted or edited.  
Topology Setup  
Conferencing Setup  
System Setup  
Network Device Monitor  
System Maintenance/Troubleshooting and Trace troubleshooting  
Create Provisioning Profiles  
Create Software Updates  
Network device admin  
Create configuration profiles for phones  
Create software updates for phones  
When areas are enabled:  
Assign RealPresence Resource Manager users to manage areas  
Create areas  
Place Entities in areas  
View and/or modify all areas |
| Auditor             | Endpoint Usage Report  
Network Usage Report  
Alert Level Settings  
System Log Files  
Audio Log Files  
Log Settings |

<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 Scheduler (sometimes called basic scheduler) role can schedule conferences. They do so using the conference templates defined for them. 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>Same with the basic schedulers except that 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 View-only Scheduler 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 conference page and they have access to the Guest Book.
When view-only schedulers log into the RealPresence Resource Manager system, the system displays the conference page and it is the only menu item to which they have access.

**Operator Role, Responsibilities, and Menus**

The **Operator** role enables businesses to offer high-touch customer service for video conferencing. Users 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.

**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 using scheduled management.
- Update endpoints using scheduled management.

When device administrators log into the RealPresence Resource Manager system, the system displays the system Dashboard.

**Auditor Role, Responsibilities, and Menus**

The **Auditor** role enables security-conscious companies to separate system administration functions from system auditing functions. It provides an extra 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.
- View and download system log files.
- Respond to audit log alerts.
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.

Customized Roles and Responsibilities

The RealPresence Resource Manager system provides you almost unlimited flexibility in defining and redefining roles, but for simplicity and clarity, Polycom recommends 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.

<table>
<thead>
<tr>
<th>Permission Set</th>
<th>Permitted Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrators Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Directory Setup</td>
<td>Create users</td>
</tr>
<tr>
<td></td>
<td>Create user groups</td>
</tr>
<tr>
<td></td>
<td>Create a guest book</td>
</tr>
<tr>
<td></td>
<td>Create a room</td>
</tr>
<tr>
<td></td>
<td>Create a machine account</td>
</tr>
<tr>
<td></td>
<td>Create address books</td>
</tr>
<tr>
<td>Site Topology Setup</td>
<td>Site Topology</td>
</tr>
<tr>
<td></td>
<td>Sites</td>
</tr>
<tr>
<td></td>
<td>Site-Links</td>
</tr>
<tr>
<td></td>
<td>Network Clouds</td>
</tr>
<tr>
<td></td>
<td>Territories</td>
</tr>
<tr>
<td></td>
<td>Reports&gt; Site Statistics</td>
</tr>
<tr>
<td></td>
<td>Reports &gt; Site-Link Statistics</td>
</tr>
<tr>
<td>Conferencing Setup</td>
<td>Direct Conference Templates</td>
</tr>
<tr>
<td></td>
<td>Conference Settings</td>
</tr>
<tr>
<td></td>
<td>Favorites</td>
</tr>
<tr>
<td>System Setup</td>
<td>System configuration under Admin</td>
</tr>
<tr>
<td></td>
<td>Endpoint Monitor</td>
</tr>
<tr>
<td></td>
<td>Endpoint Image Management</td>
</tr>
<tr>
<td>System Maintenance/Troubleshooting</td>
<td>Dashboard and troubleshooting utilities -- without wireshark trace.</td>
</tr>
<tr>
<td>System Maintenance Troubleshooting - Trace</td>
<td>Dashboard and troubleshooting utilities -- with wireshark trace</td>
</tr>
<tr>
<td>Assign User to managed Area</td>
<td>Edit user or user group for assigned area.</td>
</tr>
<tr>
<td>Permission Set</td>
<td>Permitted Tasks</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Place entities in Areas</td>
<td>Edit MCU for assigned area.</td>
</tr>
<tr>
<td>Provision Profiles</td>
<td>Endpoint provisioning profile management and ACL control.</td>
</tr>
<tr>
<td>Network Device Monitor</td>
<td>Network device monitor function.</td>
</tr>
<tr>
<td><strong>Operator Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Endpoint Admin</td>
<td>Endpoint management, control provisioning and software update for scheduled Endpoints.</td>
</tr>
<tr>
<td>Network Device Admin</td>
<td>Network Device management.</td>
</tr>
<tr>
<td>Schedulable resource monitor</td>
<td>Monitor MCU and RealPresence DMA pool status.</td>
</tr>
<tr>
<td>Conference operator</td>
<td>View, manage, and control all conferences in system. Have no permission for scheduling conferences.</td>
</tr>
<tr>
<td>Report Operator</td>
<td>Manage the reports in system (view and export reports).</td>
</tr>
<tr>
<td>View and edit all areas</td>
<td>View and edit the areas.</td>
</tr>
<tr>
<td><strong>Scheduler Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Schedule conferences (view-only)</td>
<td>View all scheduled conference in system. Have no permission for scheduling conferences.</td>
</tr>
<tr>
<td>Schedule conferences (basic)</td>
<td>View and schedule new conference of the user account, but can't select bridge or change the conference settings in the template.</td>
</tr>
<tr>
<td>Schedule conferences (advanced)</td>
<td>View and schedule new conference of the user account and change conference settings for scheduled conferences.</td>
</tr>
<tr>
<td><strong>Auditor Permissions</strong></td>
<td>Getting system logs</td>
</tr>
</tbody>
</table>
Working with Groups

Groups provide a more efficient and consistent use of the RealPresence Resource Manager system. You can use groups to assign roles and provisioning profiles to sets of users rather than to individual users.

Local Groups

The RealPresence Resource Manager system enables you to add local groups (that is, groups added manually to the system) and associate them with provisioning profiles, roles, and address books. 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) or included in an address book. The remaining group information is pulled from the enterprise directory.

Managing Groups

In the RealPresence Resource Manager system, only users assigned the Administrator role can manage groups.

Add a Local Group

You can create local groups. You must have the Administrator role to manage groups.

To add a local group:

1. Go to User > User Groups.
2. In the User Groups page, click Add +.
3. Complete the **General Info** section of the **Add Group** dialog.

4. Click **Filter** to search for the users and groups to add to this local group.

5. 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.

6. Click **Update**.
   
The group appears in the **User Groups** list. It is identified as a LOCAL group.

### Assign Address Books to User Groups

### User Group Settings

Configure the settings for user groups.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>User 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>Enterprise Directory Viewable</td>
<td>Indicates if the group is displayed in the endpoint directory</td>
</tr>
<tr>
<td></td>
<td>Do not mark</td>
</tr>
<tr>
<td>Assigned Area</td>
<td>If your RealPresence Resource Manager system has areas enabled, you can</td>
</tr>
<tr>
<td></td>
<td>choose to assign this user to an area that you manage.</td>
</tr>
<tr>
<td><strong>Associated Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Available Roles</td>
<td>The list of roles defined to the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Selected Roles</td>
<td>The list of roles that you assign users when adding them to the system. Users</td>
</tr>
<tr>
<td></td>
<td>have all of the permissions associated with all of the roles assigned to them</td>
</tr>
<tr>
<td></td>
<td>(that is, permissions are cumulative).</td>
</tr>
<tr>
<td><strong>Address Book</strong></td>
<td></td>
</tr>
<tr>
<td>Address Book</td>
<td>See Assign Address Books to User Groups.</td>
</tr>
<tr>
<td><strong>Group Members (Local Users Only)</strong></td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>Search for finding users</td>
</tr>
<tr>
<td>Search Results</td>
<td>The users and groups identified to the system that you can add to the local</td>
</tr>
<tr>
<td></td>
<td>group. This list can include both local and enterprise users and groups.</td>
</tr>
<tr>
<td>Group Members</td>
<td>The users and groups selected as part of the group</td>
</tr>
</tbody>
</table>

### Import Enterprise Groups

When you import an enterprise group, you can edit the group, user roles, and specify whether or not the group directory is viewable. You can also search for enterprise users.
You must have the Administrator role to manage groups.

- 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.

To import one or more enterprise groups:

1. Go to User > User Groups.
3. Click Filter and type all or part of the group name (with wildcards) in the Search Available Groups field, and press Search.
   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.

Edit a Group

You can edit both local or enterprise 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.
You must have the Administrator role to manage groups.
The Group Members section is only available for Local groups.

To edit a local or enterprise group:

1. Go to User > User Groups.
2. In the User Groups page, select the group you want to edit and click Edit .
3. As required, edit the General Info, Associated Roles, and Group Members sections of the Edit Local Groups dialog.
4. Click Update.

Delete a Group

You can delete a local or enterprise group. Deleting an enterprise group only deletes it from the system, not the enterprise directory. You can re-import an enterprise group if necessary.
You must have the Administrator role to manage groups.

To delete a local or enterprise group:

1. Go to User > User Groups.
2 In the **User Groups** page, select the group you want to delete and click **Delete**.

3 Click **OK** to confirm the deletion.

   The group is deleted from the system.
Managing Meeting Rooms

The RealPresence Resource Manager system enables 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 enables you to add local rooms (that is, rooms added manually to the system) and associate them with endpoints. To dynamically manage the endpoint associated with a local room, associate each room in the system with a machine account.

View the Rooms List

You can view a list of rooms. To edit or view additional details about a room, you can select it and choose an action.

To view the rooms list:

» Go to User > Rooms.

The Rooms list appears. It can be filtered by Site.

Search for a Room

You can search the list of rooms. When searching for a room that is in the enterprise directory, you must use the search field with which the room was created. For example, if the enterprise directory room was created using the Last Name field in the enterprise directory, you must use that field within the RealPresence Resource Manager system. In such an example, if you use the First Name field, the search will not return the correct result.

To search for a room:

1. Go to User > Rooms.
2. On the Rooms list, click Add .
   The Add New Room dialog box appears.
3. Click the Find Room in Enterprise Directory button.
4. In the Room Name field, type in the first few characters of the room name.
   The system does a prefix search of the appropriate fields.
5 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.

### 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.

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 enables 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.

**To add a local room:**

1. Go to **User > Rooms**.
2. On the **Rooms** page, click **Add**.
   The **Add New Room** dialog box appears.
3. Complete the **General Info** and **Associated Endpoints** sections of the **Add New Room** dialog box.
4. In the **SIP Dial String Reservations** section, click **Add** to add SIP dial string reservations.
5. On the **SIP Dial String Reservations** dialog, select the user’s **Endpoint Type** and enter the appropriate dial string for **SIP URI**, then click **OK**.
   The dial strings appear in the list below.
   By default, the same SIP URI is used for all endpoints that belong to the same user. If the user has multiple endpoints and you want a different SIP URI for each device type, enter the dial strings for one endpoint type at a time and click **OK** each time on the **SIP Dial String Reservations** dialog.
6. In the **H323 Dial String Reservations** section, click **Add** to add H323 dial string reservations.
7. On the **H323 Dial String Reservations** dialog, select the user’s **Endpoint Type** and enter the appropriate dial string for **E164** and **H323 ID**, then click **OK**.
   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 **OK** each time on the **H323 Dial String Reservations** dialog.
8. Click **Update**.
   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.

### Room Information

The table shows the room information in the RealPresence Resource Manager system records.
Managing Meeting Rooms

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.

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 enables 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.

To add an enterprise room:

1. Go to User > Rooms.
2. On the Rooms list, click Add  
   The Add New Room dialog box appears.
3. To find a room in the enterprise directory:
   a. Click the Find Room in Enterprise Directory button.
   b. Click click Filter  

### Field Description

<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></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 <strong>Restricted</strong> 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 email address of the room administrator.</td>
</tr>
<tr>
<td>Assign Area</td>
<td>Select an area to which to assign this room.</td>
</tr>
<tr>
<td></td>
<td>This field is visible only when Areas are enabled.</td>
</tr>
<tr>
<td></td>
<td>A user can view area-specific information only for an area 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.</td>
</tr>
</tbody>
</table>
c In the **Room Name** field, type in the first few characters of the room name. The system does a prefix search of the appropriate fields.

d **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.

e **Select the room of interest and click Define Details.**

4 **Complete the General Info, Associated Endpoints, SIP Dial String Reservations, and H323 Dial String Reservations sections of the Add New Room dialog box.**

5 **Click Update.**

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

You can edit a room, including its name, dial string reservations, and so on.

**To edit a room:**

1. Go to **User > Rooms.**
2. In the **Rooms** list, select the room you want to edit and click **Edit.**
3. Edit the **General Info, Associated Devices, SIP Dial String Reservations, and H323 Dial String Reservations** sections of the **Edit Room** dialog box.
4. **Click Update.**

### Delete a Room

You can delete a room. When you delete a room, you are also asked if you want to delete the dial strings (aliases) associated with the room.

**To delete a room:**

1. Go to **User > Rooms.**
2. In the **Rooms** list, select the room you want to delete and click **Delete.**
3. In the **Delete Room** dialog, click **OK.**

The room is deleted from the RealPresence Resource Manager system.
System Configuration

System configuration contains the RealPresence Resource Manager server settings, system security, certificates, enterprise directory integration, multi-tenancy, area, and system redundancy management.
Securing the System

You can configure various security features of your system. You can determine how you want to work with security certificates, make the system’s operating system more secure, as well as configure session management and password settings.

Security settings work in tandem with the security certificates you have installed. For example, if you enable strict TLS settings, you will need to add the required certificates to your system and systems that need to communicate with the RealPresence Resource Manager system, such as endpoints the system manages or network devices.

Managing Security Baselines

Security baselines are snapshots of the system's security settings that you can save in order to apply or audit at a later time.

The system comes with two baselines ready for use:

- **Standard Security Baseline Settings**
  
  The Standard Security Baseline is applied by default. You can customize any security settings after Standard Security Baseline is applied

- **High Security Baseline Settings**

  You should use the high security baseline settings only when you require maximum levels of security. When you select the high security baseline, the SSH Access is set to Disabled Permanently. This setting becomes read-only and you cannot change it back.

Unless you require a maximum level of security, you should use the Standard Security Baseline Settings. You can audit your security settings against a saved baseline to easily view any security settings you have changed since that baseline was created.

You can also apply an existing baseline to your RealPresence Manager system. However, if you try to apply a security baseline that will disallow a configured function, the application will fail to update security settings that are in conflict with configured system functions.

How you use security settings is dependent on how you have configured certificates for your system.

Create a Security Baseline

When you add a security baseline, you save a list of the currently configured system security settings for the system. Creating a security baseline allows you to easily audit your system against the baseline to see what changes were made since the baseline was created.
To create a new security baseline:

2. Click Add.
3. In the Add Baseline dialog, enter a Name and Description for your baseline.
4. Click OK.

View a Security Baseline

You can view the configuration of an existing security baseline.

To view a security baseline:

2. Select a baseline.
3. Click View Details.
   - The configuration information will appear on the right.
4. Expand each item to view the settings.

Edit a Security Baseline

You can edit the security baselines that you created. The High Security Baseline Settings and Standard Security Baseline Settings cannot be edited.

To delete a security baseline:

2. Select a baseline.
3. Click Edit.
4. Modify the Name and Description if needed.
5. Click OK to save the changes.

Delete a Security Baseline

You can delete the security baselines that you created. The High Security Baseline Settings and Standard Security Baseline Settings cannot be deleted.

To delete a security baseline:

2. Select a baseline.
3. Click Delete.
4. Click OK to confirm the deletion.
Apply Security Baseline

After you apply an existing security baseline to your system, the security options of the existing baseline will take effect. You do not need to configure the settings one by one. After applying an existing security baseline, you can customize security options; for example, TLS and system hardening.

When you apply a security baseline, the system will reboot.

To view a security baseline:
2. Select an existing baseline.
3. Select More > Apply Baseline.
   The system will reboot.

Audit Your System Against a Security Baseline

You can audit your security settings at any time. Auditing your system against a saved security baseline allows you to easily see how your settings differ from the settings within that security baseline.

To audit your security settings using a security baseline:
2. Select a security baseline from the list.
3. Click More > Audit Baseline to view the Audit Baseline Results.
4. Click Close.

Audit Baseline Results

The Audit Baseline Results dialog lists the security settings that differ from the selected Security Baseline and includes the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Lists the current security setting that differs from the selected security baseline.</td>
</tr>
<tr>
<td>Baseline Value</td>
<td>Lists the value of the security setting that is stored in the selected security baseline.</td>
</tr>
<tr>
<td>Current Setting Value</td>
<td>Lists the current value of the listed security setting.</td>
</tr>
</tbody>
</table>
Configure Secure Communication

You can configure secured communications for the following protocols: HTTP, LDAP, FTP, SMTP, SNMP, Global Directory Services (GDS), and Outbound Telnet.

To configure secure communication:

1. Go to Admin > Management And Security > Secure Communication.
2. Enable secured communication settings for the protocols.

Related Topics

Enable Integration with the Enterprise Directory Server
Secure Communication Protocols

Secure Communication Protocols

Enable the secured communication protocols.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP: Enforce Secured http</td>
<td>Enabling this option may impact services using HTTP, such as scheduled endpoint management, remote endpoint reboot, and MCU management using HTTP.</td>
</tr>
<tr>
<td>LDAP: Enforce Secured LDAP</td>
<td>After enabling secured LDAP, you must select either LDAPS or StratTLS as Security Level when configuring Enterprise Directory integration. See Enable Integration with the Enterprise Directory Server on how to configure Security Level.</td>
</tr>
<tr>
<td>FTP: Enforce Secured FTP</td>
<td>Enabling this option may impact services using FTP, such as backing up the system using FTP.</td>
</tr>
<tr>
<td>SMTP: Enforce Secured SMTP</td>
<td>Enabling this option may impact services using SMTP.</td>
</tr>
<tr>
<td>SNMP: Enforce Secured SNMP v3</td>
<td>Enabling this option may impact services using SNMP v3. SNMP v2 will be disabled if you enable this option.</td>
</tr>
<tr>
<td>Disable GDS (Global Directory Service)</td>
<td>After GDS is disabled, Polycom Global Address Book cannot be used.</td>
</tr>
<tr>
<td>Disable Outbound Telnet</td>
<td>After outbound telnet is disabled, the server controlled endpoint dialing out and hanging up functions will be impacted.</td>
</tr>
</tbody>
</table>

Configure TLS Settings

You can configure how the RealPresence Resource Manager deals with security certificates. How you set up your TLS settings determines the level of security you have for your system.

If you choose to use the High Security Baseline Settings, most of these settings cannot be changed.
For example, you can require all clients attempting to access the system to present a certificate.

After you install a full PKI chain, you should delete the self-signed certificates of any system on which the self-signed certificate has been replaced with a CA signed certificate. Self-signed certificates are not allowed when the system is in maximum security mode.

To configure TLS settings:

2. Configure the TLS Settings.
3. Click Update.

Related Topics

Supported Ciphers
Security Certificates
TLS Settings

**TLS Settings**

The table explains the TLS settings.
### Securing the System

#### Polycom, Inc.

### Related Topics

**Supported Ciphers**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cipher Mode | You can choose from the following cipher modes:  
• **Standard Ciphers** When you choose Standard Ciphers, all the supported Ciphers can be used. See for all the supported Ciphers.  
• **Weak Ciphers** The supported Ciphers with key size less than 128 bits.  
• **Strong Ciphers** The supported Ciphers with key size equal to or more than 128 bits.  
  When you use the **High Security Baseline Settings**,Cipher mode is set to Strong Ciphers and cannot be changed. |
| Validate Certificates for Connections from Clients | This setting requires all clients (endpoints, peripherals, and users accessing the RealPresence Resource Manager system web interface over an encrypted protocol such as SSL or TLS) to send identity certificates in order to access the system.  
You must have at least one CA certificate installed if you want to validate external certificates.  
If you are using the UC-APL security settings, this setting is enabled by default, but can be configured. During First Time Setup you should uncheck this setting; it will be checked later after completing First Time Setup (this can help avoid connection problems from occurring during initial configuration). |
| Validate Certificates for Connections to Servers | This setting requires all servers (other Polycom systems such as the RealPresence DMA system or the RealPresence Collaboration server as well as third-party integrations), accessing the RealPresence Resource Manager system web interface over an encrypted protocol such as SSL or TLS) to send identity certificates in order to access the system.  
You must have at least one CA certificate installed if you want to validate external certificates.  
Mark the **Verify Hostname** setting if you want to verify the host name (IP address) of the server. With **Verify Hostname** enabled, IP address will be used to validate the CA certificate of RealPresence Resource Manager. Therefore the SAN must contain the IP address of the server (RealPresence Resource Manager), otherwise, verifying host name will fail. |
| Enable FIPS -140 | When you enable FIPS-140, **Strong Ciphers** and **Validate Certificates for Connections to Servers** are automatically checked and cannot be disabled.  
You cannot use TLSv1.2 for Microsoft Active Directory connections if you enable FIPS-140. |
| Check Revocation Status | This option is available only when you check the **Validate Certificates for Connections from Clients** or **Validate Certificates for Connections to Servers** check boxes. When enabled, RealPresence Resource Manager will check if the CA is revoked or not. |
| Enable CBC Ciphers | Enable CBC ciphers. |
| Enable Static Ciphers | Enable static ciphers. |
Configure System Hardening

Operating system hardening is the process of securely configuring the system against the unauthorized access, intruders, hackers, and other security vulnerabilities. System hardening makes the computer system more reliable, secure, efficient, and gives the optimized performance.

System hardening may also disable features that you want to use. Select these options carefully.

To configure System Hardening:

1. Go to Admin > Management and Security > System Hardening.
2. Configure the settings for System Hardening.

System Hardening

The table explains the settings for system hardening.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable NIDS</td>
<td>Allows the Network Instruction Detector System to run.</td>
</tr>
<tr>
<td>Ignore Redirect Flag</td>
<td>Redirect flags will be ignored.</td>
</tr>
<tr>
<td>Allow ICMP (ping) responses</td>
<td>You can choose to disallow the RealPresence Resource Manager to respond to ping messages.</td>
</tr>
<tr>
<td>Respond to ICMP (ping) requests with</td>
<td>If you choose to allow the server to respond to ping requests, you can configure a Destination Unreachable message.</td>
</tr>
<tr>
<td>Destination Unreachable message</td>
<td></td>
</tr>
<tr>
<td>Allow traces for troubleshooting</td>
<td>Troubleshooting traces are not encrypted, you can disable these.</td>
</tr>
<tr>
<td>Allow Linux console access</td>
<td>You can disable Linux console access to the RealPresence Resource Manager server. This setting disables console access for all users.</td>
</tr>
<tr>
<td>Disable Root User Login</td>
<td>Root user login is disabled.</td>
</tr>
<tr>
<td>SSH Access</td>
<td>Allow users to use SSH to access RealPresence Resource Manager system.</td>
</tr>
<tr>
<td></td>
<td>Note: The Disable Permanently option is irrevocable.</td>
</tr>
<tr>
<td>Lock Bios</td>
<td>(Appliance Only) Bios access is protected by complicated password after enable Lock Bios.</td>
</tr>
</tbody>
</table>

Session Security and User Access

You can control various aspects of user sessions with the RealPresence Resource Manager system’s web interface.
Change the System User Interface Timeout and Number of Sessions

You can modify the length of the user interface timeout as well as set up parameters for how many active sessions are allowed.

To change the system user interface timeout and number of sessions:

1. Go to Admin > Management and Security > Session Management.
2. Configure the settings on the Session Management page.
3. Click Update.

Session Management Settings

Configure the settings on the Session Management page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealPresence Resource Manager user interface timeout (minutes)</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</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. This setting is available only when RealPresence Resource Manager is in maximum security mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></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>
<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>

Disable Linux Console Access

By default, users can access the RealPresence Resource Manager system through the Linux console. You can disable this ability.

To disable Linux console access:

1. Go to Admin > Management and Security > System Hardening.
2. Clear the Allow Linux console access option.
3. Click Update.
Enabling and Editing Log in Banners

The log in banner is the message that appears when users attempt to access the system. Users must acknowledge the message before they can log in. By default, the long banner field on the Banner Configuration page displays the required Standard Mandatory Notice and Consent Provision for systems operating in a maximum security environment. The short banner field displays a shortened version of this same notice.

The long banner is used for the RealPresence Resource Manager system log in banner. The RealPresence Resource Manager system provides several sample long banners. You can use these banners as is or edit them to create a custom long banner. The RealPresence Resource Manager system provides a single short banner, which you can also customize. If you customize the banners, remember that the long banner message may contain up to 5000 characters. The short banner message may contain up to 1315 characters.

Enable Banner

You must enable banner to show the message when you log into the system.

To enable banner:
1. Go to Admin > Management and Security > Session Management.
2. Check the Enable Banner check box.
3. Click Update.

Edit Banner

The Banner Configuration page allows users assigned the Administrator role to customize the long and short login banners.

To edit the login banners:
1. Go to Admin > Management and Security > Banner Configuration.
2. From the Message drop-down menu, select the sample banner that most suits your needs.
3. Edit the banner as needed. If you edit one of the existing banners, the Message menu selection changes to Custom.
4. Click Update.

Set Local Account Lockout and Timeout

You can configure failed login thresholds as well as how long a local user account can be locked out after a failed login.

To set local account lockout and timeout:
2 Configure the settings on the User Account Configuration page.
3 Click Update.

User Account Configuration Settings
Configure the settings on the User Account Configuration page.

<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>

Using Whitelist for IP Access
You can configure a whitelist of IP addresses that will be allowed to access the RealPresence Resource Manager system's web interface or SNMP information. Once you enable the list, only IP addresses on the list will be allowed to access the web interface or SNMP information.

Create a Whitelist to Manage Access
Add a whitelist to allow only specified IP addresses to access the RealPresence Resource Manager system's web interface or SNMP information.

To configure a list of IP addresses:
1 Navigate to Admin > Management and Security > Management Access Settings.
2 In the Whitelist screen, select the Enable Management Access Settings check box.
3 Click Add .
4 In the Add Whitelist dialog, specify the IP address(s) to be included.
   You can specify IP addresses individually or as a range. If IPv6 is enabled, you can enter either an IPv4 address or range or an IPv6 address or range.
5 Click Update to save the IP address to the whitelist.
   Repeat these steps to continue adding IP addresses or ranges of IP addresses until finished.
6 Click Update on the main page to save your whitelist.
Securing the System

Disable Management Access Settings

After you disable Management Access, all IP addresses will be allowed to access the RealPresence Resource Manager system's web interface or SNMP information.

To disable a list of IP addresses:

2. In the Whitelist screen, cancel the Management Access Settings check box.
3. Click Update to save your changes.

Set Sensitive Information Disclosure

You can choose not to display some detailed error messages and build number by configuring Information Disclosure.

To configure the settings for information disclosure:

2. Check Generalize Error Message to hide detailed error information or uncheck Build Number Display to hide build numbers on the GUI.

Set Password Requirements

If you have been assigned the Administrator role, you can configure password requirements for local users. You can 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 > Password Requirements.
2. Configure the settings on the Password Requirements page.

Password Requirement Settings

Configure the settings on the Password Requirements page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Management</td>
<td></td>
</tr>
<tr>
<td>Minimum length (characters)</td>
<td>Specify the number of characters a password must contain. Possible value is 8 to 15.</td>
</tr>
<tr>
<td>Minimum changed characters</td>
<td>Specify the number of characters that must be different from the previous password. Possible value is 1 to 4.</td>
</tr>
<tr>
<td>Minimum password age (days)</td>
<td>Specify how frequently a password can be changed. Possible value is 1 to 30.</td>
</tr>
</tbody>
</table>
Securing the System

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum password age (days)</td>
<td>Specify at what age a password expires. Possible value is 30 to 180.</td>
</tr>
<tr>
<td>Password warning interval (days)</td>
<td>Specify when users start to see a warning about their password expiration.</td>
</tr>
<tr>
<td></td>
<td>Possible value is 1 to 7.</td>
</tr>
<tr>
<td>Reject previous passwords</td>
<td>Specify how many of the user’s previous passwords the system remembers</td>
</tr>
<tr>
<td></td>
<td>and won't permit to be reused. Possible value is 8 to 16.</td>
</tr>
</tbody>
</table>

**Password Complexity**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowercase letters</td>
<td>Specify the number of lowercase letters (a-z) that a password must contain.</td>
</tr>
<tr>
<td></td>
<td>Possible value is 1 or 2.</td>
</tr>
<tr>
<td>Uppercase letters</td>
<td>Specify the number of uppercase letters (A-Z) that a password must contain.</td>
</tr>
<tr>
<td></td>
<td>Possible value is 1 or 2.</td>
</tr>
<tr>
<td>Numbers</td>
<td>Specify the number of digit characters (0-9) that a password must contain.</td>
</tr>
<tr>
<td></td>
<td>Possible value is 1 or 2.</td>
</tr>
<tr>
<td>Special characters</td>
<td>Specify the number of non-alphanumeric keyboard characters that a password</td>
</tr>
<tr>
<td></td>
<td>must contain. Possible value is 1 or 2.</td>
</tr>
<tr>
<td>Maximum consecutive repeated characters</td>
<td>Specify how many sequential characters may be the same. Possible value is</td>
</tr>
<tr>
<td></td>
<td>1 to 4.</td>
</tr>
</tbody>
</table>

**OS Account Password Policy**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the above rules to the OS account</td>
<td>When enabled, all the password rule configuration is applied to OS password.</td>
</tr>
</tbody>
</table>

**Conference PIN Code**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length</td>
<td>Specify the number of characters a PIN code must contain. Possible value is</td>
</tr>
<tr>
<td></td>
<td>4 to 9</td>
</tr>
<tr>
<td>Maximum length</td>
<td>Specify the maximum number of a PIN code. Possible value is 9 to 16.</td>
</tr>
<tr>
<td>Maximum consecutive repeated characters</td>
<td>Specify how many sequential characters may be the same. Possible value is</td>
</tr>
<tr>
<td></td>
<td>1 to 2.</td>
</tr>
</tbody>
</table>

**Reset System Passwords**

You can configure random passwords for the RealPresence Resource Manager internal system processes (including database and other internal 3rd party software services, excluding OS accounts and RealPresence Resource Manager application users). Use these options only when you require the maximum security.

After resetting passwords, you need to re-integrate RealPresence Resource Manager and the RealPresence DMA systems for network topology synchronization. You may need to re-setup Polycom RealAccess data collection features.

**To reset system passwords:**

1. Go to **Admin > Management and Security > Reset System Passwords**.
2 Click the **Reset System Passwords** button.
3 Click **OK**.

## Encryption

The following table lists the product capabilities that are supported but not necessarily required. Requirements vary based on the customer environment.

**Product Capabilities**

<table>
<thead>
<tr>
<th>Application</th>
<th>Encryption Function</th>
<th>Description</th>
<th>Protocol Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Confidentiality</td>
<td>Management API: Server provides a local management interface over encrypted HTTP( used for Web GUI, Rest API and Provisioning)</td>
<td>SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Confidentiality</td>
<td>AD integration: Allows product to retrieve enterprise directory entries from a Microsoft active directory-compatible server over an encrypted LDAPs channel; Directory service: provides AD-compatible directory service for devices.</td>
<td>SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XMPP</td>
<td>Confidentiality</td>
<td>Presence service: Allows product to post its current presence state to a configured XMPP server and obtain presence information for other users/devices from XMPP server, using an encrypted TLS channel; Note: This product also supports the XMPP Chat service.</td>
<td>SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Stored Data</td>
<td>Confidentiality</td>
<td>System Backup/Restore encryption</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Upgrade file encryption</td>
<td></td>
</tr>
<tr>
<td>Remote Password</td>
<td>Confidentiality</td>
<td>It is used to store the password of the account for login remote entity.</td>
<td>N/A</td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>Confidentiality</td>
<td>SNMP Agent: Allows SNMP console applications to connect to the product over an encrypted SNMPv3 channel.</td>
<td>SNMPv3</td>
</tr>
</tbody>
</table>

Polycom, Inc.
Security Certificates

User certificates between systems within your video conferencing environment (such as servers and endpoints) to build a trust/authentication and to support encryption. Certificates confirm that the servers within your infrastructure can communicate and have the option to encrypt the data. 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).

The CA, or certificate authority, is a single, centralized authority such as an enterprise’s IT department or a commercial certificate authority that each computer on the network is configured to trust. Each server on the network has a public certificate that identifies it. When a client connects to a server, the server shows its signed public certificate to the client. The certificate authority signs the public certificates of those servers that clients should trust. Trust is established because the certificate has been signed by the certificate authority (CA), and the client has been configured to trust the CA.

How Certificates Work

Before installing any certificates or configuring Online Certificate Status Protocol (OCSP) responder settings, you must configure how the RealPresence Resource Manager system will use certificates. This is done by configuring your TLS settings.

TLS settings also specify if client systems (endpoints and systems who access the RealPresence Resource Manager system user interface) are required to present certificates for authentication. Determine the degree in which you want to use certificates within your deployment and configure the settings appropriately.

Configure TLS Settings

Accepted Certificates

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. Typically, this default certificate is not 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 be configured with at least one root CA certificate, and a digital certificate signed by the CA that identifies the RealPresence Resource Manager system.

However, you will often need additional CA certificates to allow the system to properly validate a received certificate. Work with your network administrator to gather all required certificates needed in the environment. Here is a simple checklist:

- RealPresence Resource Manager Identify Certificate - created by the system via the Certificate Signing Request (CSR) (see Certificate Signing Requests) and signed by a CA within your network infrastructure.
- CA certificate for the CA that signs the RealPresence Resource Manager Identity Certificate
- A root CA certificate - this is the certificate for the root of the CA hierarchy.
- The CA certificates for all intermediate CAs between the root CA and the CA that signs the RealPresence Resource Manager identity certificate.
- The certificate used to validate responses from the OCSP responder.

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>
<tbody>
<tr>
<td>PEM (Base64-encoded ASCII text)</td>
<td>PKCS #7 standard P7B file</td>
<td>Certificate chain containing:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A signed certificate for the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The CA’s public certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sometimes intermediate CA certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Upload file or paste into text box.</td>
</tr>
<tr>
<td>CER (single certificate)</td>
<td>PEM (Base64-encoded ASCII text)</td>
<td>Upload file or paste into text box.</td>
</tr>
<tr>
<td>Certificate text (can be PKCS#7(P7B)</td>
<td></td>
<td>Encoded certificate text copied from CA’s email or secure web page.</td>
</tr>
<tr>
<td>or a single certificate)</td>
<td></td>
<td>Paste into text box.</td>
</tr>
</tbody>
</table>
Security Certificates

Certificate Signing Requests

The initial RealPresence Resource Manager system configuration permits 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. You need to create a certificate signing request for the RealPresence Resource Manager system and submit it to a certificate authority to be signed.

Although it is common for a system to be identified by any number of digital certificates, each signed by a different CA, the RealPresence Resource Manager system currently only supports a single identity certificate.

Requirements for Certificate Signing Request

When you choose to use security certificates with your video infrastructure environment, you need to generate a CSR (Certificate Signing Request) for the Certificate Authority (CA) you are using.

Since the RealPresence Resource Manager system uses this single certificate for both TLS client and TLS server connections, it is important that the certificate template used on the CA enable both "clientAuth" and "serverAuth" use in the "Extended Key Usage" (EKU) field of the certificate. Related bits in the "Key Usage"
extension should be set accordingly per RFC 5280 guidance. Work with the administrator of the CA to assure this.

When you create a certificate signing request (CSR) from RealPresence Resource Manager system, the system not only populates the CSR with the data that you enter in the Certificate Information dialog, but it also populates some of the CSR’s subject alternative name (SAN) fields. This information is not visible in the Certificate Information dialog.

The RealPresence Resource Manager system generates a CSR containing all of the information in the following table for your configuration. You cannot edit or remove any of the fields, including those listed in the Optional Fields column. If your CA cannot accept a CSR that includes all of this information, you must generate the CSR and certificate manually using at least the data in the Required Fields column for your configuration. If you include the fields listed in the Optional Fields column, users can access the system using an abbreviated name without authentication errors.
The RealPresence Resource Manager system only uses the DNS format for SAN values, even though some values are IP addresses.

**Required and Optional CSR SAN Fields**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Required Fields</th>
<th>Optional Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-server System</td>
<td>• SAN-DNS – Fully Qualified Domain Name (FQDN)</td>
<td>• SAN-DNS – Host short name</td>
</tr>
<tr>
<td></td>
<td>• SAN-DNS – System IP address (Ipv4)</td>
<td>• SAN-DNS – Ipv6 address, if used</td>
</tr>
<tr>
<td></td>
<td>• Country Name (two-letter code)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State or Province Name (full name)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Organizational Name(s) (one per line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Key Size</td>
<td></td>
</tr>
<tr>
<td>Local Redundant System</td>
<td>• Common Name – Fully Qualified Domain Name (FQDN) of Virtual IP Address</td>
<td>SAN-DNS – Virtual host short name</td>
</tr>
<tr>
<td></td>
<td>• SAN-DNS – FQDN of Virtual IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Country Name (two-letter code)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State or Province Name (full name)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Organizational Name(s) (one per line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Key Size</td>
<td></td>
</tr>
<tr>
<td>Geo-Redundant System</td>
<td>• Common Name – Fully qualified domain name (FQDN) of the virtual host name</td>
<td>SAN-DNS – Server 1 short name</td>
</tr>
<tr>
<td></td>
<td>• SAN-DNS – FQDN of the virtual host name</td>
<td>SAN-DNS – Server 2 short name</td>
</tr>
<tr>
<td></td>
<td>• SAN-DNS – First NIC IP address of server 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SAN-DNS – First NIC IP address of server 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Country Name (two-letter code)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State or Province Name (full name)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Organizational Name(s) (one per line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Email address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Key Size</td>
<td></td>
</tr>
</tbody>
</table>

**Create a Certificate Signing Request**

You should create a certificate signing request after you have completed the network configuration of your system.

**To create a certificate signing request:**


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:

- 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 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 Request Data** dialog, enter the identifying information for your RealPresence Resource Manager system and click **OK**.

A **File Download** dialog appears.

4 In the **File Download** dialog, click **Save**.

5 In the **Save As** dialog, 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 email text, email attachments, or be available on a secure web page.

---

**Certificate Request Data**

Enter the identifying information for your RealPresence Resource Manager system in the **Certificate Request Data** dialog.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Algorithm</td>
<td>You can select either SHA256 or SHA1.</td>
</tr>
<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 and 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>Optional: Subdivision (ASCII only) of the enterprise at which the server is located. Multiple values are permitted, one per line.</td>
</tr>
<tr>
<td>Common Name</td>
<td>The FQDN (fully-qualified domain name) of the system (read-only), as defined in the network settings.</td>
</tr>
<tr>
<td>E-mail Address</td>
<td>Email address (ASCII only) for a contact at the enterprise.</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>Your CA must support at least six SAN fields.</td>
</tr>
</tbody>
</table>
Installing Certificates

You must configure your network settings before you install certificates.

If you update your network settings (for example, if you change FQDN or change the network protocol IPv4 to IPv6), you must reconfigure certificates for your system.

Before changing server certificate, ensure that FIPS mode is disabled. You may lose the RealPresence Resource Manager GUI access after changing server certificate with FIPS enabled.

Install a Certificate

Before installing a certificate or certificate chain provided by the certificate authority, be sure that you received the certificate or certificate chain in one of the following forms:

- A PFX, P7B, or single certificate file that you’ve saved on your computer.
- PEM-format encoded text that you received in an e-mail or on a secure web page.

Installing or removing certificates requires a system restart. When you install a certificate, the change is made to the certificate store immediately, but the system will not recognize or use the new certificate until it restarts and reads the changed certificate store.

To install a signed certificate that identifies the RealPresence Resource Manager system:

2. Click Install Certificates.

A warning appears stating that changes made to the certificates will require a system restart to take effect.

3. In the Install Certificates dialog, do one of the following:

   - If you have a PKCS#12, 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. PKCS #12 is not supported when the RealPresence Resource Manager system is in maximum security mode or when Strong Ciphers (FIPS) mode is being used.
   - If you have PEM-format text, copy the certificate text, click Paste Certificate, and paste it into the text box at the bottom of the dialog. You can paste multiple PEM certificates one after the other.

4. 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.

5. Verify that the new signed certificate has replaced the default self-signed certificate:

   - In the list of certificates, select the RealPresence Resource Manager certificate and click View Certificate Details.
   - In the Certificate Details dialog, verify that the information in the Issued To sections matches the FQDN of the RealPresence Resource Manager and the certificate from the certificate authority and that the information in the Issued By section matches the expected name of the certificate authority.
   - Click Close to close the dialog.
Use the same procedure to install other certificates as needed (intermediate CA certificates, root CA certificates, certificate used to validate OCSP responses). You need to install all CA certificates that are part of the chain of trust for any client or server identity certificate that the system may be presented and be required to validate on any of its external connections. Work with your network administrator to determine this list.

**View Certificates and Certificate Details**

You can view currently installed certificates and certificate details, including expiration dates.

**To view the list of installed certificates:**

2. 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 RealPresence Resource Manager self-signed certificate. When other certificates are installed, they will display along with the server identity certificate.
3. To view more information about a certificate, select the certificate and click *View Certificate Details* from the *More* drop-down list. The *Certificate Details* dialog appears.
4. Use the arrows to reveal or hide information. Click *Close* when you are done.

**Related Topics**

- Certificate Management Information
- Certificate Details

**Certificate Management Information**

The *Certificate Management* page has the following information.

<table>
<thead>
<tr>
<th>Field</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>Alias</td>
<td>The certificate name as assigned by the CA.</td>
</tr>
<tr>
<td>Common Name</td>
<td>This is most often the fully qualified domain name of the server to which</td>
</tr>
<tr>
<td></td>
<td>the certificate has been issued. If the certificate identifies a client</td>
</tr>
<tr>
<td></td>
<td>(trusted peer) it might contain the name of a user or the name of an endpoint.</td>
</tr>
</tbody>
</table>

Polycom, Inc. 461
Removing Certificates

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, you must first install new CA certificates and the identity certificate must be replaced.

There are two kinds of certificate removal:

- Removing the certificate of a Trusted Root CA so that the system no longer trusts certificates signed by that certificate authority.
- Removing the signed certificate currently in use so that the system reverts to using the default self-signed certificate.

Removing a signed certificate also removes the certificate of the Trusted Root CA that signed it, along with any intermediate certificates provided by that certificate authority.

Installing or removing certificates requires a system restart and terminates all active conferences. When you install or 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.
For your convenience, you’re not required to restart and apply a change immediately. This permits you to perform multiple installs or removals before restarting and applying the changes. But when you’re finished making changes, you must select **Restart to Apply Saved Changes** to restart the system and finish your update. Before you begin, make sure there are no active conferences and you’re prepared to restart the system when you’re finished.

**Remove a Trusted Root CA’s Certificate**

You can remove a trusted root CA certificate so that the system no longer trusts certificates signed by that certificate authority.

**To remove a Trusted Root CA’s certificate:**

1. Go to **Admin > Management and Security > Certificate Management**.
2. In the certificates list, select the certificate you want to delete.
3. Click **Delete Certificate**.
4. When asked to confirm, click **OK**.
   A dialog informs you that the certificate has been deleted.
5. Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.

**Remove a Signed Certificate and Revert to Default Self-Signed Certificate**

Removing the signed certificate currently in use as the certificate so that the system reverts to using the default self-signed certificate.

Removing a signed certificate also removes the certificate of the Trusted Root CA that signed it, along with any intermediate certificates provided by that certificate authority.

**To remove a signed certificate and revert to the default self-signed certificate:**

1. Go to **Admin > Management and Security > Certificate Management**.
2. In the certificates list, select the certificate to which you want to revert.
3. Select **Revert to Legacy VVX Certificate** from the **More** drop-down list.
4. When asked to confirm, click **OK**.
   A dialog informs you that the system has reverted to a self-signed certificate.
5. Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.
6. After the system restarts, log back in, return to **Management and Security > Certificates Management**, and verify that the system has reverted to the default self-signed certificate:
   a. In the list of certificates, select the default certificate.
   b. Click **View Certificate Details** from the **More** drop-down list.
      The **Certificate Details** dialog appears.
c Confirm from the information under **Issued To** and **Issued By** that the default self-signed certificate has replaced the CA-signed certificate.

d Click **Close** to close the dialog.

**Regenerate a Default Self-Signed Certificate**

You need to update your certificate(s) whenever you make network configuration changes such as changing the host name or IP of your RealPresence Resource Manager system.

After you generate a default certificate, you will need to restart your system.

**To regenerate a self-signed certificate:**

1. Go to **Admin > Management and Security > Certificate Management.**
2. Click **Regenerate Resource Manager Certificate** from the **More** drop-down list.
3. Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.
4. After the system restarts, log back in, return to **Management and Security > Certificates Management**, and verify that the system has reverted to the default self-signed certificate by confirming the information under **Issued To** and **Issued By** that the default self-signed certificate has replaced the CA-signed certificate.

**Revert to a Legacy VVX Certificate**

Some versions of the Polycom VVX systems rely on the self-signed certificate that comes installed with the RealPresence Resource Manager system.

The legacy self-signed certificate is deleted automatically when you import a CA certificate chain. However, if you need to revert to a self-signed certificate scenario for your systems, you will need to revert back to the Legacy VVX Certificate.

The Legacy VVX certificate supports only 1024-bit key RSA.

**To revert to the Legacy VVX certificate:**

1. Go to **Admin > Management and Security > Certificate Management.**
2. Select **Revert to Legacy VVX Certificate** from the **More** drop-down list.

**OCSP Settings**

The RealPresence Resource Manager system supports using OCSP (Online Certificate Status Protocol) to verify the status of a certificate. This is an alternative to manually uploading CRLs (Certificate Revocation Lists). If your network does not include an OCSP responder, the RealPresence Resource Manager system parses individual certificates for a CRL Distribution Point URL. There is no need to upload a CRL to complete your certificate validation.

When configuring the RealPresence Resource Manager system to use an OCSP responder, you can either use the default OCSP information that is included in the certificates you receive or explicitly define the
OCSP responder location. You should only define an explicit OCSP responder location if your deployment relies on a global OCSP responder.

After you configure OSCP settings, you will need to restart your system.

To configure OSCP settings for your certificate(s):

2. Select the Enable Online Certificate Status Protocol (OCSP) check box if your organization's PKI includes OCSP responders for revocation checking.
   This check box is automatically enabled when your system is in maximum security mode.
3. Use the OCSP Certificate drop-down list to select one of the installed certificates to use to verify OCSP responses. Which certificate to use depends on your OSCP server configuration. Consult with your security administrator.
4. Depending on your security configuration, you can enter the URL of an OCSP Responder location to use. During first-time setup, it is recommended that you leave this field blank. This can ensure that you don't have connection problems during initial configuration.
   a. If OCSP is enabled and no responder URL has been specified:
      俊 If the certificate contains an OCSP URL it will be used to check revocation. The OCSP URL is found in the certificate's AIA field.
      俊 If the certificate doesn't contain the OCSP URL then if the certificate contains a CDP it will be used to check revocation.
      俊 If the certificate doesn't contain a CDP revocation check fails and certificate isn't trusted.
   b. If OCSP is enabled and a global responder URL has been specified the global responder is used to check revocation.
      俊 If the global responder cannot be contacted and the certificate contains a CDP it will be used to check revocation.
      俊 If the certificate doesn't contain a CDP revocation check fails and the certificate isn't trusted.
5. Click Verify OSCP Configuration.
   The system verifies that the OSCP configuration is correct. If the OSCP URL as well as the OSCP certificate, the configuration will also be verified as correct.
6. Click Save OSCP Configuration.
   The system saves this configuration.
7. After making any changes, you must reboot the system.

When you enable OCSP and install a CA certificate whose Authority Information Access (AIA) or CRL Distribution Points (CDP) pointing to a URL outside the corporate network, the RealPresence Resource Manager system accesses the URL to validate the certificate. If there's no network, a warning message prompts saying that "The certificate revocation status is undetermined", but you can continue without validating the certificate.
Configuring Multi-Tenancy

The RealPresence Resource Manager system supports multi-tenancy with its areas feature. Multi-tenancy enables you to use the system 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, and 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 system 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.

The Areas feature of the RealPresence 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 to ensure scalability and efficient use of resources. Setting up the RealPresence Resource Manager system for multi-tenancy should use the following best practices:

- RealPresence Resource Manager system 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 dynamic provisioning when areas are enabled. Other methods of endpoint provisioning are not supported. See Admin Config Provisioning Profiles.
- RealPresence DMA systems, Polycom VBP systems, RealPresence Access Director systems, 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 RealPresence 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 system. 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.

**Admin Config Provisioning Profiles**

**Working within a Multi-Tenancy Environment**

When using the RealPresence Resource Manager system’s 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.

**User Roles within a Multi-Tenancy Environment**

When you enable 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 RealPresence Resource Manager tasks for all areas. RealPresence 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.

**Area Roles**

An area role delegates RealPresence 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 an 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 RealPresence 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.

### 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. A user with a system role sees all address books, but a user with only an area role sees only address books that belong to the areas that the user belongs to or to areas in which the user manages.
A user that views the contents of an address book that has members from multiple areas can view only those members that belong to areas the user has access to. A user with a non-area-specific role can see address book members from all areas, but a user with only area-specific roles can see only members that belong to the areas the user manages.

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 available address book members 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 areas, he can add users from any area that he manages to the user group. Remember that system administrators 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 RealPresence Resource Manager system ensures that a user and the 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.

A warning message notifies the logged-in user about the change and provides opportunity to cancel the operation. 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 RealPresence 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 RealPresence Collaboration Server (RMX) system that is explicitly assigned to the area to which the operator belongs or the scheduler can use a RealPresence Collaboration Server (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 scheduler 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 system 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 RealPresence 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.

11 Add billing codes, if preferred.

Create Areas for Tenants

You can create a new area for each new tenant.

To create areas:

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).

Setting up Area Management

The RealPresence Resource Manager provides you flexibility when setting up how to manage an area.

Managing 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.

Managing 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, they cannot perform the tasks associated with their role. Area users can be configured to manage more than one area, see Assign Users to Manage an Area(s).

Assigning 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.

The Administrator role is the only pre-defined role that can add or edit conference templates.

Resources 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

Resources Belong to One or More Areas (or no Area)

Resources that can be associated with one or more areas or no areas are:

- RealPresence DMA Pool Orders

Adding 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.
Configuring 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.

Site Topology for Multiple Tenants

Associating Billing Codes with Conferences

The RealPresence Resource Manager system supports associating a billing code with a conference. This feature is only available when areas are enabled.
You can define billing codes within an area that can then be assigned to conferences. When an area scheduler creates a conference within an area that includes billing codes, the scheduler can associate a billing code with that conference.

Billing codes are included in CDRs. This enables you to track how much each department (billing code) within an area is using video resources. Service providers can use this information to create billing breakdowns for their tenants.

Users with the Administrator role can create new billing codes for an area. Users with the area scheduler or area operator role are allowed to associate a billing code with a conference when the schedule the conference.

### Add a New Billing Code

Billing codes are supported when areas are enabled. You can add a billing code(s) to an area when you create an area or when you edit an existing area.

**To add or edit a new billing code:**

1. Navigate to Admin > Areas.
2. Click Add to add a new area or select an area in the list and click Edit.
3. In the Edit an Area dialog, click Billing Code.
4. On the Billing Code page, do the following:
   a. In the Billing Code field, enter the billing code you want to use.
   b. Enter a description for the billing code.
   c. Click Apply.
5. Click OK.

### Delete a Billing Code

Users with the administrator role can delete billing codes.

**To delete a billing code:**

1. Navigate to Admin > Areas.
2. Select an area in the list and click Edit.
3. In the Edit an Area dialog, click Billing Code.
4. On the Billing Code page, do the following:
   a. Select a billing code.
   b. Click Delete.
5. Click OK.

**Note:** To clear the billing code fields after an existing billing code in the list has been selected, click Apply.
Associating a Billing Code with a Conference

When creating a new conference, you can select a billing code after you select conference participants.

Viewing Billing Code Information

The Conference Usage Report now includes billing code information for each conference. Billing code information is also included in conference information sent to the Polycom RealPresence DMA system and the Polycom RealPresence Collaboration Server (RMX) systems.

When monitoring conferences, you can also filter conferences by billing code.
Managing Areas

You can manage areas on the RealPresence Resource Manager GUI.

Enable Areas

Before you can manage area and use area related features, you need to first enable areas.

To enable areas:

1. Go to Admin > Areas.
2. Select More > Configure Areas.
3. In the Configure Areas dialog, mark the Enable Areas Functions in Resource Manager check box.
4. Click OK and log in again.

Add an Area

You can add an area. Before adding an area, review the Create Areas for Tenants topic.

To add an area:

1. Go to Admin > Areas > Areas.
2. Click Add to add a new area.
3. Click Set Resource Manager System Logo.
4. In the Set Resource Manager System Logo dialog box, browse to a file to upload and click Upload.
5. When the upload is complete, click OK.
6. Click Set CMA Desktop Logo.
7. In the Set CMA Desktop Logo dialog box, browse to a file to upload and click Upload.
8. When the upload is complete, click OK.
10. On the Billing Code page, do the following:
    a. Click Add to add a new billing code.
    b. In the Billing Code field, enter the billing code you want to use.
    c. Enter a description for the billing code.
d. Click OK.

11. Click OK.

**Related Topics**

Create Areas for Tenants

**Edit an Area**

You can edit an area.

**To add an area:**

1. Navigate to Admin > Areas.
2. Select an area to edit and click **Edit**.
3. Click **Set Resource Manager System Logo**.
4. In the **Set Resource Manager System Logo** dialog box, browse to a file to upload and click **Upload**.
5. When the upload is complete, click **OK**.
6. Click **Set CMA Desktop Logo**.
7. In the **Set CMA Desktop Logo** dialog box, browse to a file to upload and click **Upload**.
8. When the upload is complete, click **OK**.
9. Click **Billing Code and** do the following:
   a. In the **Billing Code** field, enter the billing code you want to use.
   b. Enter a description for the billing code.
   c. Click **Apply**.
10. Click **OK**.

**Viewing 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>Area 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. Select the area information from the More drop-down list.
4. The following View actions are available. The details you can view from each action is dependent on the type of resource it is.

Remove 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:

To delete an area and all of its resources:

1. Backup your data.
2. Click Delete to delete the area and its resources.

To delete the area, but keep all of its resources in the system:

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:
2. Edit the resources you would like to keep and reassign them to other areas or to no area.
3. Backup your data.
4. Click Delete to delete the area and its remaining resources.

Move the Contents of an Area

If you wish to delete the area, but keep all of its resources in the RealPresence 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.
To move an area’s resources to another area:

1. Go to Admin > Areas.
2. Select the area.
3. Click More > Move Contents.
4. Select the available area from the Move the objects associated with the area being deleted to area drop down list.
5. Click OK.

**Deleting an Area and its Resources**

If you no long need an area and its resources, you can delete them from the RealPresence Resource Manager system.

Before deleting an area, you must manually un-assign any network devices and sites 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 canceled.
- 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:

- RealPresence 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.

If an area is still in use when you try to delete it (a conference being scheduled, a resource being added), the area may not be completely deleted. If you receive an **Unable to Delete Area** message, it will detail resources that still need to be deleted. You will need to manually delete or re-assign these resources and then rerun the Delete Area action. Before deleting an area, you must manually un-assign any network devices and sites from the area. You should also verify that there are no ongoing conferences or area users involved in a conference belonging to another area.
Customizing the Area Logos (system and CMA Desktop) for the Area

You can customize the logos that a RealPresence Resource Manager system’s 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.

**Customize the System Log for an Area**

You can customize the system log for an area.

To customize the system logo for an area:

1. Go to Admin > Area > Area Logos.
2. Select an area of interest and click More > Set Resource Manager System Logo.
3. In the Resource Manager System Logo dialog box, browse to a file to upload and click Upload.
4. When the upload is complete, click OK.

**Customize the CMA Desktop Logo**

You can customize the CMA Desktop logo for CMA Desktop users within the area.

To customize the CMA Desktop logo for CMA Desktop users within the area:

1. Go to Admin > Area > Area Logos.
2. Select an area of interest and click More > Set CMA Desktop Logo.
3. In the Resource Manager System Logo dialog box, browse to a file to upload and click Upload.
4. When the upload is complete, click OK.
System Redundancy

A redundant RealPresence Resource Manager system configuration offers high availability with higher reliability and greater call success by ensuring that your system is always available.

The redundancy configuration requires two RealPresence Resource Manager system servers. The two servers are running as active or standby modes. For both servers in redundancy, system services are provided via the first NIC and the redundancy connection must go through the second NIC. The service interface of RealPresence Resource Manager is directed through the first NIC and the redundant interface is the second NIC.

How Redundancy Works

A redundant configuration (high availability) includes two servers: a primary server and a redundant server.

The primary server is actively involved in managing endpoints and monitoring conferences. It actively responds to network traffic routed to it. In a normal operational state, the primary server is the active server.

In a failover state, the redundant server is the active server.

The active or inactive server communicates every 1000 milliseconds using a private IP address and port 5405. If the inactive server does not receive 4 consecutive heartbeats (i.e., four seconds) 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 running on the primary server 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 RealPresence Resource Manager system user interface.

Also, the failover to the redundant server occurs seamlessly because the endpoints are registered with either an FQDN or a virtual IP address, which remains constant. However, endpoints that are dynamically managed will lose the connection as the provisioning service will stop for approximately eight minutes.

During a failover:

- Users logged into the RealPresence Resource Manager system user interface are disconnected and returned to the main RealPresence 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. The order is:
  - Database Service
System Redundancy

- Apache Service
- Jserver
- Device Manager
- Site Topology Service
- Dial Rules Service
- Global Address Book Service
- Polycom Cascade Service
- Polycom Scheduler Service
- GateKeeper Service
- Openfire Service

A system failover usually takes approximately 8 minutes for all provisioning services to continue.

Once a failover to a redundant server occurs, the redundant server manages all system operations until another failover occurs or if the administrator switches back to the original primary server via the Switch Server Roles function in the RealPresence Resource Manager system user interface.

The RealPresence Resource Manager system does not automatically switch to the primary server when the primary server becomes available. An administrator may Switch Server Roles if needed.

Configuration Considerations for Redundancy

Consider the following:

- 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.
- Ensure each system uses the same RealPresence Resource Manager software version.
- (Appliance) Ensure each system uses the same server type for R620 and R630. For example, use two Polycom Rack Server 620 servers. R230 and R220 can be each other’s redundant server.
- You can use as much HDD space as exists on the smallest system.
- Ensure both systems are up and running before you configure redundancy.
- After you install a certificate on your primary server, the secondary server will be synchronized to use the same certificate.
- If configuring redundancy on an existing system, Polycom recommends making a system backup before configuring redundancy.
- When adding redundancy to an existing system, be sure to set up redundancy on the existing server first. If you set up redundancy in the wrong order, data will be lost.
- You cannot change the system name or domain name after configuring redundancy.

Interoperability Considerations for Redundancy

Please consider the following interoperability issues when using a redundant configuration:
● After a system failover, RealPresence Mobile and RealPresence Desktop users must re-login before they can search their directories.

● You cannot dynamically provision a RealPresence Access Director system using a virtual FQDN. If you are using a geographic redundant configuration, you need to manually add and manage your RealPresence Access Director system.

● You cannot dynamically manage Polycom VVX 1500 systems using a virtual FQDN.
  ▶ For software updates, you need to manually update Polycom VVX endpoints.
  ▶ For provisioning, create a specific network profile for Polycom VVX systems. Do not use the Default Directory Server or Default Presence Server. Instead leave those check boxes unmarked, and specify the primary IP address.

### Local versus Geographic Redundancy

Depending on your network requirements, you can use either local redundancy or geographic redundancy. The license requirements are the same for both configurations.

● You can use local redundancy when both servers are in the same geographic location and accessible to each other via VLAN or crossover cable/

● You can use geographic redundancy when your servers are in two geographically distant sites.

Configuring Local System Redundancy

Geographic System Redundancy.

### Managing a Redundant System

After you have configured your system for redundancy, you can track system failovers and manually initiate a system failover.

#### Manually Failover to a Redundant Server

In a redundant configuration, you can manually initiate a failover or let the system automatically fail over from the primary server to the redundant server when necessary.

The **Switch Server Role** option is not available if the inactive server is not available.

To manually initiate a failover:

1. Log into the system using the virtual IP address for local redundancy or using the virtual FQDN for geographic redundancy.

2. Go to **Admin > Server Settings > Redundant Configuration**.

3. On the **Redundant Configuration** page, click **Switch Server Role**.
   
   The system initiates a failover to the other server.
Track System Failovers

You can monitor how and when the system has failed over. The RealPresence Resource Manager system provides detailed messages about the time and reason for a system failover.

You can also view system failover information in the System Alerts pane and on the System Dashboard (Redundancy pane).

To view the time and reason of the last system failover:

1. Log into the RealPresence Resource Manager system using the virtual IP address for local redundancy or using the virtual FQDN for geographic redundancy.
2. Go to Admin > Server Settings > Redundancy Configuration.
3. View the read-only information for the time and reason of the failover.

Failover Information

The table describes the failover reasons.

<table>
<thead>
<tr>
<th>Failover Reason</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public NIC is down.</td>
<td>The network interface card went down on the active server.</td>
</tr>
<tr>
<td>Gateway is unreachable.</td>
<td>The active system could not reach the network gateway either because the network cable is unplugged or for network issues external to the system.</td>
</tr>
<tr>
<td>Web application is down.</td>
<td>The application service on the active server stopped and the web interface cannot be reached.</td>
</tr>
<tr>
<td>Database is down.</td>
<td>The system database went down on the active server.</td>
</tr>
<tr>
<td>Site topology database is down.</td>
<td>The site topology database went down on the active server (Opends database).</td>
</tr>
<tr>
<td>Manual failover.</td>
<td>The failover was manually initiated by the administrator.</td>
</tr>
<tr>
<td>Active server not responding.</td>
<td>The active server could not be reached.</td>
</tr>
</tbody>
</table>

Discontinue Redundancy

In some circumstances, you may need to discontinue redundancy. You can discontinue redundancy whether or not both servers are accessible. However, the steps for each circumstance are different.

If only one server can be accessed, discontinue redundancy on that server first. Discontinue redundancy on the other server after it can be accessed.

To discontinue a redundant configuration:

1. Log into the system using the virtual IP address for local redundancy or using the virtual FQDN for geographic redundancy.
2. Go to Admin > Server Settings > Redundant Configuration.
3 On the **Redundant Configuration** page, click **Reset Redundant Configuration**.
   If both servers are accessible, the two servers restart as single servers and you can skip the rests steps.
   If only one server is accessible, the primary system restarts as a 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** for local redundancy or using the **virtual FQDN** for geographic redundancy.
5 Go to **Admin > Server Settings > Redundant Configuration**.
6 On the **Redundant Configuration** page, click **Reset Redundant Configuration**.
   The system restarts as single server.

**Restore Redundancy**

In some circumstances, you may need to restore redundancy from a backup archive.

**To restore redundancy:**
1 Discontinue the redundancy.
2 Restore the system on the primary server from a backup archive.
3 Re-set up the redundancy.

**Related Topics**

- System Backup and Recovery
Configuring Local System Redundancy

A local redundant system configuration (high availability) 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 for both the service interface and redundant interface. If you do not configure an IP address for the redundant interface, the redundant interface IP will be automatically generated as 169.254.*.*

A locally redundant RealPresence Resource Manager system configuration requires two RealPresence 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.

See System Redundancy for details on how to perform fail-overs and for more information on how redundant systems work.

Optional: Perform a System Backup

If you are setting up redundancy for an existing RealPresence Resource Manager system that has already been active, you should first backup your existing system. See Creating System Backups for details.

Ensuring the Servers Can Communicate

You need to be sure that your two servers can communicate over the local network.

- The active/inactive servers communicate over a dedicated private network using a crossover LAN cable physically connected from the two servers via the Redundant NIC of each server, or over a VLAN connection using the IP address of the Redundant NIC on each server.
- The IP addresses for the redundant interfaces of the respective servers MUST be on the same subnet.

Network Configuration Requirements on Both Servers

Basic settings for the two servers must match.

- Be sure they are both configured to the same NTP server.
Configure Local System Redundancy

- Ensure both servers are configured with a Redundant Interface that defines an IP address for the redundant NIC of each server. The default IP addresses can be used. The IP addresses for the redundant interfaces of the respective servers MUST be on the same subnet.

Make note of the IP addresses used for the redundant interfaces. You’ll need to enter them when you configure your system for redundancy.

Enable the Root User Login and SSH Access

The RealPresence Resource Manager system requires SSH Access and the root user login to configure redundancy. These settings are disabled by default. You need to change them before configuring redundancy.

To enable the root user login and SSH Access:

1. Go to Admin > Management and Security > System Hardening.
2. Cancel the Disable Root User Login check box.
3. Select Enable in the SSH Access drop-down list.
4. Click Update.

Optional: Change the Redundant Interface IP Address

You can change the default IP address and subnet mask used for the redundant interface (the 2nd NIC of the server).

You will need to restart your system after you changing the default IP address and subnet mask for the redundant interface.

To edit the redundant interface:

1. Go to Admin > Server Settings > Network.
2. Configure these settings on the Redundant Interface tab of the Network page, as necessary.
3. Update the IP address for the network interface used for redundancy if needed.
4. Click Save Settings.
5. Restart the server.

Network Interface IP Address

The table explains the IP addresses for the network interface used for redundancy.
To set up redundancy for your environment:

1. Log into the primary server using the physical IP address.
2. Go to Admin > Server Settings > Redundant Configuration.
3. Enter the IP Settings for the redundant configuration.
4. Click Submit. If you have changed the root password, (with the help of Polycom Global Services), you'll be prompted to enter the root password.
   Both systems reboot.
5. Verify that you can access your system(s) using the virtual IP address.

**Related Topic**

Enable the Root User Login and SSH Access.

**IP Settings for Local Redundant Configuration**

The table explains the IP settings for the redundant configuration.

<table>
<thead>
<tr>
<th>IP Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP</td>
<td>Enter the Virtual IP that will be used to access the system.</td>
</tr>
<tr>
<td>Virtual Host Name</td>
<td>Enter the value of the FQDN for the virtual IP</td>
</tr>
</tbody>
</table>
License a Local Redundant System

To license a redundant system for an Appliance Edition, you need to have a license for both servers within your configuration. However, both licenses need to be installed by accessing your configured system using the virtual IP address.

If you use Virtual Edition servers to set up redundant system, you only need one license for the primary server. The secondary server doesn't need license.

When your servers work in offline mode, you must upload the same license file to the primary and secondary servers.

To license a redundant system (Appliance Edition only):

1. Request both a license for the primary server and a license for the secondary server as described in Request a Software License File.
2. Use your browser to navigate to the virtual IP address of the RealPresence Resource Manager system and log in.
4. Click Update License.
5. Follow the instructions on the Update License dialog and be sure you have a backup copy of your initial license file.
6. Click Choose File and navigate to the primary license file you requested.
7. Click Preview and then click Apply.
8. Click Update License again.
9. Follow the instructions on the Update License dialog.
10. Click Choose File and navigate to the secondary license file you requested.
11. Click Preview to verify that the license is correct.
12. Click Apply.

Related Topics

Request a Software License File
Provisioning Considerations

When you provision endpoints to use the RealPresence Resource Manager system for directory services and presence, you need to use the virtual IP address. If you do not use the virtual IP address, endpoints will not have the correct information for directory and presence services if a fail over occurs.
Geographic System Redundancy

A geographic redundant RealPresence Resource Manager system configuration offers higher reliability and greater call success by ensuring that your system is always available.

A geographic redundant RealPresence Resource Manager system configuration requires two RealPresence Resource Manager system servers and four physical IP addresses as well as a DNS-defined FQDN address dedicated to external access and endpoint registration.

Network Requirements for a Geographic Redundant System

Geographic redundancy allows you to use two RealPresence Resource Manager systems in disparate network locations to support redundancy.

Geographic redundancy requires the following:

- Set up a common FQDN for services.
- A dedicated Data Center link with the following requirements for the heartbeat network connection:
  - TCP/UDP ports must not be changed by NAT or other network devices between the two servers.
  - Network Latency < 200ms
  - Network Bandwidth > 100Mbit/s
  - Network Packet Loss = 0 percent

Redundancy services may not work if the above requirements for the network connection are not met.

Optional: Perform a System Backup

If you are setting up redundancy for an existing RealPresence RealPresence Resource Manager that has already been active, you should first backup your existing system. See Create a System Backup Manually for details.

Perform Network Configuration on Both Servers

Install both of your RealPresence Resource Manager systems as described in the Polycom RealPresence Resource Manager Getting Started Guide. Basic settings for the two servers must match.

- Be sure they are both configured to the same NTP server.
Geographic System Redundancy

- Ensure both servers are configured with a Service Interface that defines an IP address for the first NIC of each server.
- Ensure both servers are configured with a Redundant Interface that defines an IP address for the second NIC of each server.
- Make note of the IP addresses used for the redundant interface. You’ll need to enter them when you configure your system for redundancy.

Enable the Root User Login

The RealPresence Resource Manager system requires the root user login to be enabled in order to configure redundancy. This setting is disabled by default. You need to change it before configuring redundancy.

To enable the root user login:

1. Go to Admin > Management and Security > System Hardening.
2. Ensure the Disable Root User Login check box is unmarked.
3. Click Update.

Configure DNS for the Redundant Servers

In addition to the required DNS steps for non-redundant configurations, you need to create a zone delegation for the servers within your geographically redundant system. You need to set up a common Fully Qualified Domain Name (FQDN) for the redundant servers, using the service interface IP addresses for each server (first NIC).

You’ll use the FQDN you create to connect to the RealPresence Resource Manager system once you have configured it for redundancy.

To ensure DNS for your geographically-redundant system:

1. Add an NS records for each of the redundant servers, using the service interface IP (first NIC).
2. Configure DNS zone delegation for your redundant services.
3. Make note of the FQDN that you create. That FQDN is used to access your system.

Configure the System for Redundancy

You configure both systems for redundancy via the primary server. The both servers are configured for redundancy after you have configured the primary system redundancy.

The RealPresence Resource Manager system requires SSH Access and the root user login to configure redundancy. These settings are disabled by default. You need to change them before configuring redundancy.
To set up redundancy for your environment:

1. Log into the primary server using the physical IP address.
2. Go to Admin > Server Settings > Redundant Configuration.
3. Enter the IP Settings for the redundant configuration.
4. Click Submit. If you have changed the root password (with the help of Polycom Global Services), you’ll be prompted to enter the root password.
   Both systems reboot.
5. Verify that you can access your system(s) using the common FQDN address.

**Related Topic**

[Enable the Root User Login and SSH Access.](#)

### IP Settings for Geo-redundant Configurations

The table explains the IP Settings for the geo-redundant configurations.

<table>
<thead>
<tr>
<th>IP Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP</td>
<td>For geo-redundancy configurations, you can leave this field blank. You must use an FQDN to access a geographically redundant configuration.</td>
</tr>
<tr>
<td>Virtual Host Name</td>
<td>The hostname that corresponds to the virtual IP address. Enter the FQDN you created here.</td>
</tr>
<tr>
<td>Local Server Redundant IP Address</td>
<td>This is the IP address of the redundant interface of the local server. It is read automatically and is readonly. This IP address should point to the second NIC on your primary server.</td>
</tr>
<tr>
<td>Peer Server Redundant IP Address</td>
<td>The IP address of the redundant interface IP of the peer server in your configuration. This IP address should point to the second NIC on your redundant server.</td>
</tr>
</tbody>
</table>

### License a Geographic Redundant System

To license a geographic redundant system, you must have a license for both servers within your configuration. However, you must install both licenses by accessing your configured system using the common FQDN.

When your servers work in offline mode, you must upload the same license file to the primary and secondary servers.

> When you add devices to the RealPresence Resource Manager system to license them, you need to use the common FQDN. If you don’t use the common FQDN, the devices may not have the correct information for license services.

**To license a redundant system (Appliance Edition only):**

1. Request a both a license for the primary server and a license for the secondary server.
2 Use your browser to navigate to the common FQDN of the RealPresence Resource Manager system and log in.

3 Navigate to Admin > Server Settings > Licenses.

4 Click Update License.

5 Follow the instructions on the Update License dialog and be sure you have a backup copy of your initial license file.

6 Click Choose File and navigate to the primary license file you requested.

7 Click Preview and then click Apply.

8 Click Update License again.

9 Follow the instructions on the Update License dialog.

10 Click Choose File and navigate to the secondary license file you requested.

11 Click Preview to verify that the license is correct.

12 Click Apply.

**Related Topics**

- Reclaim Software Client Licenses
- Request a Software License File

**Provisioning Considerations**

When you provision endpoints to use the RealPresence Resource Manager system for directory services and presence, use the common FQDN. If you don’t use the common FQDN, endpoints don’t have the correct information for directory and presence services if a failover occurs.
System Maintenance

This section provides an introduction to the Polycom® RealPresence Resource Manager system maintenance.
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.

**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.
- Monitoring system health and performing the recommended regular maintenance.
- Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. Should the need arise, Polycom Global Services personnel may ask you to use these tools.
- Upgrading the system when upgrades/patches are made available.

**Related Topics**

- Recommended Regular Maintenance
- System Maintenance and Troubleshooting
- Change the System User Interface Timeout and Number of Sessions

**Administrative Best Practices**

Read Polycom 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.
- Before you reconfigure, install an upgrade, or restore a backup, manually create a new backup of the system settings. You can then restore 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 enables 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 system operates efficiently and diagnose any issues that may arise in the future. Proper system time is also essential for accurate audit and CDR data, as well as system redundancy.

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

Read Polycom recommendations for auditing best practices.

● Unless otherwise instructed by Polycom Global Services, configure system 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 system 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).

Related Topics
Managing Audit Log Files

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.

Tracking System Alerts

You can track system alerts via email to remotely monitor the RealPresence Resource Manager system performance.

Related Topics
Configuring Alert Settings.
Creating Backup Archives

Polycom recommends that you regularly create backups of your RealPresence Resource Manager system. See Create a System Backup Manually for details.

General System Health and Capacity Checks

On the Dashboard, you can see various information about the system. See System Dashboard for details.

Exporting CDR

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.
System Reports

The RealPresence Resource Manager system provides various reports that you can view and export. Use these reports to identify return on investment, troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls.

View 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.

2. Click View Chart.

3. In the Site Name list, select the site(s) to chart.

4. In the Y-Axis list, select the statistic(s) to chart.

5. 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 Statistics

The table explains the Site Statistics report.

<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>Specifies the total bandwidth of the currently active calls.</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>
</tbody>
</table>
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.

2. Click View Chart.

3. In the Site Name list, select the site(s) to chart.

4. In the Y-Axis list, select the statistic(s) to chart.

5. In the Data Limit field, enter the time frame in minutes for which to chart the data. The default is 60 minutes.

6. The charts are dynamically updated for your selections. The site-links are displayed in the same order as the site-link grid.

### Site Link Statistics

The table explains the Site Link Statistics.

<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>
</tbody>
</table>
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 Reports > Report Administration.
2. In the Report Administration page, enter the number of days for the Retention Period for Conference and Endpoint CDRs.
3. Click Save Settings.

Schedule Archives of the CDR Report

You can schedule archives of CDR reports to be sent to an external server for storage.

To schedule archives of CDR information:

1. Go to Reports > Report Administration.
2. In the Report Administration page, select Enable FTP of CDRs (CSV Format) and configure the settings.
3. To verify that the FTP settings are functional, click Test Archive Settings.
4. When the settings are correct, click Save Settings.

Report Administration Settings

The table explains the Report Administration Settings.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
The Endpoint Usage Report is based on the CDRs extracted from selected endpoints and includes entries for ISDN and IP calls. Calls from WebRTC participants are not recorded in CDRs.

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:

   - The Endpoint Usage Report page displays the information for the endpoints for which CDRs are available.
     - 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.
   - To restrict the report to a different time period, change the Start Date and End Date. The report is dynamically updated.

2. Click Filter ▼ to customize the report by endpoint Type, Name, IP Address, ISDN Video Number, Dial String, Site, or VIP status.
   - You can also filter on Area when areas are enabled and you manage more than one area.

3. Select the number of reports to be displayed on the page from the Items per page drop-down list.

4. To generate the Endpoint Usage report, select one or more endpoints to include in the report and go to More > Generate Report. Use the CTRL key to select multiple endpoints.

5. To select a different group of endpoints, click Change Selected, select the endpoints, and go to More > Generate Report again.
7. Click **Call Times** to see a chart that identifies the number of calls versus the start time for the calls.

8. Click **People Count** to see a chart that identifies people count for conference usage.

9. Click **Inbound** to see a chart that identifies the endpoints from which the inbound calls to the selected endpoints originated.

10. Click **Outbound** to see a chart that identifies the endpoints to which the selected endpoints called.

11. Click **Summary CDR Report** to see a grid that displays information for each of the selected endpoints that participated in calls.

   - 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**.

12. 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.

13. Click **Detail CDR Report** to see information for each of the endpoints that participated in calls.

14. To export the information, click **Download Report**.

   - Click **For endpoint_name ONLY (Excel File)** to save the report Microsoft Excel format for the selected endpoint.
   - Click **For All Selected Endpoints (CSV File)** to save the CDR report in or in CSV format.

   - Only the first 1000 lines of the report are exported to the Excel file.

15. Click **Change Selected** to return to the **Endpoint Usage Report** page to select a different endpoint.

### Related Topics

- Available Endpoint Usage Report
- Generate Endpoint Usage Report Properties
- Summary CDR Report
- Detail CDR Report

### Available Endpoint Usage Report

The table explains the available endpoint information on the **Endpoint Usage Report** page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Name</td>
<td>The registered name of the endpoint.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The registered serial number of the endpoint.</td>
</tr>
<tr>
<td>Site</td>
<td>The location at which the endpoint resides. When areas are enabled on your</td>
</tr>
<tr>
<td></td>
<td>system, this field shows a value of <strong>Restricted</strong> if you do not have</td>
</tr>
<tr>
<td></td>
<td>permission to manage the area to which the site is assigned.</td>
</tr>
<tr>
<td>Owner/Room</td>
<td>The person or room to whom the endpoint is registered.</td>
</tr>
</tbody>
</table>
Generate Endpoint Usage Report Properties

The table describes the available information when you generate the usage report for an endpoint.

<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 Details 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>

Summary CDR Report

The table describes the Summary CDR Report

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Name</td>
<td>Identifies the endpoint by name.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The registered serial number of the endpoint.</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 Total Time in Call divided by the Total Calls.</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 Total Calls.</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>

Detail CDR Report

The table describes the Detail CDR Report.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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, 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>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>Precedence Level</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>People Mins</td>
<td>The total people count for each minute of the call. For example, if there are 10 people in the meeting and the meeting lasts for 10 minutes, the total People Mins will be 100 minutes. This information is only available for room systems equipped with a Polycom EagleEye Producer or EagleEye Director camera.</td>
</tr>
<tr>
<td>People Count (call begin)</td>
<td>Number of people on the call during the first minute of the call, tracked with EagleEye Producer or EagleEye Director II. This information is only available for room systems equipped with a Polycom EagleEye Producer or EagleEye Director II camera.</td>
</tr>
<tr>
<td>People count (peak value)</td>
<td>Peak number of people participating on the call, tracked with the EagleEye Producer or EagleEye Director II camera. This information is only available for room systems equipped with a Polycom EagleEye Producer or EagleEye Director II camera.</td>
</tr>
<tr>
<td>People Count (call end)</td>
<td>Number of people participating on the call during the last minute of the call, tracked with the EagleEye Producer or EagleEye Director II camera.</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>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>
</tbody>
</table>
Generate Network Device Usage Report

You can view the operational status of system resources by instance with SNMP enabled. Monitored system resources include CPU, memory, storage, and network.

Since RealPresence Web Suite Experience Portal does not support SNMP, system resource information is not available for it.

To generate a report:

2. Select a network instance that you want to review.
3. Click More > Generate Report.
4. Select the 24 Hours or 1 Month to show the data on the right below the chart.
5. Click Download to save this report as a CSV file. The downloaded file is saved in the browser default Download folder.
6. Click Change Selected to go back to the instance list.

Related Topics

Enable SNMP for an Instance

Create Conference Usage Report

Use the Conference Usage Report option to review usage information about system conferences. Only reports for scheduled conference calls are created. Reports for ad hoc conference calls are not created.

To create a Conference Usage Report:

2. As needed, change the Start Date and End Date to select the date range for the report.
3. Select the number of reports to be displayed on the page from the Conferences per page drop-down list.
4. Select Summary Report or Detail Report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
5 Click Export as CSV File. The file is saved to the default Download folder of your browser.

**Conference Usage Report**

The table describes the available items in summary or detail report of conference usage.

<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>Conference Owner</td>
<td>Name of the conference owner.</td>
</tr>
<tr>
<td>Conference Owner ID</td>
<td>ID of the conference owner.</td>
</tr>
<tr>
<td>Conference Alias</td>
<td>Alias of the conference.</td>
</tr>
<tr>
<td>Conference Mode</td>
<td>Mode of 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></td>
<td>If the duration of the conference is less than sixty seconds, the conference duration is displayed as zero.</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>

**Create 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.

4 To create one of the conference type report charts, click the appropriate chart name below the grid. Chart choices include:

- Scheduled vs. Ad hoc: 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 system. Monitoring information will be incorrect and inconsistent.

- Scheduled: A chart that compares the number of point-to-point, multipoint, gateway, and embedded multipoint conferences.

- Scheduled vs. Executed Mins: A chart that compares the number of scheduled minutes to the number executed minutes.

- Avg Participants in Multipoint: A chart that displays the average number of participants in multipoint conferences.

- Two Person on MCUs: A chart that displays the number of point-to-point conferences hosted on an external MCU.

The selected chart dynamically appears below the grid.

5 Click Export as CSV File. The file is saved to the default Download folder of your browser.

**Conference Type Report**

The table describes the Conference Type Report.

<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>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 system, 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 system. Monitoring information will be incorrect and inconsistent.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>
<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 a RealPresence Collaboration Server (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 a RealPresence Collaboration Server (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>
SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of resources in a network.

**SNMP Framework**

The SNMP framework has three parts:

- An SNMP manager
  The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. A variety of network management applications are available for use with SNMP. It is important to note that you should understand how your SNMP management system is configured to properly configure your Polycom system SNMP transport protocol requirements, SNMP version requirements, SNMP authentication requirements, and SNMP privacy requirements. For information on using SNMP management systems, see the appropriate documentation for your application.

- An SNMP agent
  The SNMP agent is the software component within the Polycom system that maintains the data for the system and reports these data, as needed, to managing systems. The agent and MIB reside on the same system.

- A MIB
  The MIB (Management Information Base) is a virtual information storage area for network management information, which consists of collections of managed network objects. You can configure the SNMP agent for a particular system MIB. The agent gathers data from the MIB, the repository for information about system parameters and network data. Polycom systems include Polycom-specific MIBs with every system as well as third-party MIBs. Polycom MIBs are self-documenting, including information about the purpose of specific traps and inform notifications. Third-party MIBs accessible through the Polycom system may include both hardware and software system MIBs.

**SNMP Notifications**

A key feature of SNMP is the ability to generate notifications from an SNMP agent. Notifications are called as such because they are sent, unsolicited and asynchronous to the SNMP manager from the Polycom system. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to another system, or other significant events. They are generated as informs or trap requests. Traps are messages alerting the SNMP manager to a system or network condition change. Inform requests (informs) are traps that include a request for a confirmation receipt from the SNMP manager. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. However, informs consume more system and network resources. Traps are discarded as soon as they
are sent. An inform request is held in memory until a response is received or the request times out. Traps are sent only once while informs may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and network resources.

**SNMP Versions**

Polycom supports two versions of SNMP:

- **SNMPv2c**—Polycom implements a sub-version of SNMPv2. SNMPv2c uses a community-based form of security. The community of SNMP managers able to access the agent MIB is defined by an IP-based Access Control List and password.

  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**—Polycom implements the newest version of SNMP. Its primary feature is enhanced security. SNMPv3 provides secure access to systems with a combination of authenticating and encrypting packets over the network. The contextEngineID in SNMPv3 uniquely identifies each SNMP entity. The contextEngineID is used to generate the key for authenticated messages. Polycom 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.
  - Message integrity ensures that a packet has not been tampered with in transit.

**Configuring SNMP**

The RealPresence Resource Manager system uses SNMP to provide a standardized framework and a common language used monitoring and managing the system.

The RealPresence Resource Manager system incorporates the common Polycom management framework data model. This includes system-specific SNMP MIBs, support for receiving hardware traps from both servers in a redundant system, and an SNMP REST API.

Polycom provides several MIB files that contain specific to system operations as well as MIBs that track hardware operations. Hardware MIBs such as CPU temperature and so on are tracked using Dell-specific MIBs made available through the RealPresence Resource Manager system.

You can configure what version of SNMP to use as well as set up notification receivers to help you track RealPresence Resource Manager system activities.

RealPresence Resource Manager does not support configuring a context name for SNMP.
**Enable the SNMP Agent**

You can enable the system SNMP agent.

**To enable the SNMP agent:**

1. Navigate to Admin > Server Settings > SNMP Settings.
2. Select the **Enable SNMP monitoring** check box.
3. Select the **Agent Settings** tab.
4. Configure the SNMP agent settings for the connection between the RealPresence RealPresence Resource Manager system and the SNMP agent.
5. Click **Update**.

**SNMP Agent Settings**

The table explains the SNMP Agent Settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Version</td>
<td>Specifies the version of SNMP you want to use.</td>
</tr>
<tr>
<td>v2c</td>
<td>Used for standard models. Uses community-based authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>Used when you want a high security model. Requires a security user for notifications.</td>
</tr>
<tr>
<td>Transport</td>
<td>Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocols:</td>
</tr>
<tr>
<td>TCP</td>
<td>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>UDP</td>
<td>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 RealPresence Resource Manager system uses for general SNMP messages. By default, the RealPresence 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. The RealPresence RealPresence Resource Manager system has only one valid context—by default, public—which is identified by this <strong>Community</strong> name. The RealPresence RealPresence Resource Manager system will not respond to requests from management systems that do not belong to its community.</td>
</tr>
</tbody>
</table>
Add an SNMP Notification Agent

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 agent to the system:

1. Go to Admin > Server Settings > SNMP Settings.
2. Select the Notifications Setting tab.
3. Click Add to view the Add Notification Agent dialog box.
4. Configure the settings in the Add Notification Agent dialog box.
5. Click OK.

The agent appears in the Notification Agents list.

Add Notification Agent Properties

The table describes the properties available on the Add Notification Agent page.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported MIB</td>
<td>You can select from a list of RealPresence Resource Manager-specific MIBs to maintain. The MIB you select determines which TRAPs are sent to the TRAP receivers you set. GET operations are supported for both MIBs.</td>
</tr>
<tr>
<td></td>
<td>• POLYCOM_RESOURCE_SCHEDULER_MANAGEMENT</td>
</tr>
<tr>
<td></td>
<td>• POLYCOM_CMA_MIB (legacy MIB)</td>
</tr>
<tr>
<td>V3 Local Engine Id</td>
<td>For SNMPv3 only. Displays the RealPresence Resource Manager system contextEngineId for SNMPv3.</td>
</tr>
</tbody>
</table>
Add a Security User (SNMP v3 only)

When using SNMP v3, you must add security users to associate with notifications.

To add a notification user:

1. Go to Admin > Server Settings > SNMP Settings.
2. Select the User Settings tab.
3. Click Add to view the Add Notification User dialog box.
4. Configure the settings in the Add Notification User dialog box.
5. Click OK.

The user displays in the Notification Users list.

Add Notification User Properties

The table describes the properties on the Add Notification User page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification type</td>
<td>The type of notification that this agent sends to the notification receiver:</td>
</tr>
<tr>
<td></td>
<td>• Inform–The agent sends an unsolicited message to a notification receiver and expects or requires the receiver to respond with a confirmation message.</td>
</tr>
<tr>
<td></td>
<td>• Trap–The agent sends an unsolicited message to a notification receiver and does not expect or require a confirmation message.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>The version of SNMP used for this agent (v2c or v3).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security user</td>
<td>The user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>The authentication protocol used to create unique fixed-sized message digests of a variable length message.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence RealPresence Resource Manager system implements communication with authentication and privacy (the authPriv security level, as defined in the USM MIB).</td>
</tr>
<tr>
<td></td>
<td>Authentication type options:</td>
</tr>
<tr>
<td></td>
<td>• MD5–Creates a digest of 128 bits (16 bytes)</td>
</tr>
<tr>
<td></td>
<td>• SHA–Creates a digest of 160 bits (20 bytes)</td>
</tr>
<tr>
<td></td>
<td>Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.</td>
</tr>
<tr>
<td>Authentication password</td>
<td>The authentication password that's used, together with the local engine ID, to create the authentication key included in the MD5 or SHA message digest.</td>
</tr>
</tbody>
</table>
Enable SNMP for an Instance

Enabling SNMP for an instance configures the RealPresence Resource Manager system to act as an SNMP manager for that instance, receiving communications from an SNMP agent on the instance. You must enable SNMP on each RealPresence Platform component instance that you want to monitor. Then you can configure SNMP settings for the instance in the RealPresence Resource Manager system.

To configure SNMP settings for monitoring an instance:

2. Select a network instance you want to configure and click More > SNMP Settings.
3. Select the Details tab, and then click SNMP at the left of the screen.
4. Select the SNMP version.
   - The configuration selections vary depending on which SNMP version you choose.
5. Depending on the SNMP version selected, complete the applicable fields of the instance monitoring configuration.
6. Click OK to save the new settings.

Network Device SNMP Configuration

The table explains the fields in Network Device SNMP Configuration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption type</td>
<td>For SNMPv3 only. Specifies the privacy protocol for the connection between the RealPresence RealPresence Resource Manager system and the SNMP agent.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence RealPresence Resource Manager system implements communication with authentication and privacy (the authPriv security level as defined in the USM MIB).</td>
</tr>
<tr>
<td></td>
<td>Possible values for privacy protocol are:</td>
</tr>
<tr>
<td></td>
<td>• DES—Uses a 56 bit key with a 56 bit salt to encrypt the SNMPv3 packet.</td>
</tr>
<tr>
<td></td>
<td>• AES—Uses a 128 bit key with a 128 bit salt to encrypt the SNMPv3 packet.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption password</td>
<td>The password that’s used, together with the local engine ID, to create the encryption key used by the privacy protocol.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>The transport protocol to be used. At this time, RealPresence Resource Manager supports only UDP (User Datagram Protocol), not TCP.</td>
</tr>
<tr>
<td></td>
<td>UDP requires fewer network resources and is suited for repetitive, low-priority functions like alarm monitoring, although message delivery is not assured and does not always occur in the order in which messages are sent.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which the SNMP manager communicates.</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.

### Download MIBs

The RealPresence Resource Manager system enterprise MIB relates information about the system. The information is divided into these categories:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community</td>
<td>For SNMPv2c only. Functions as a global password for accessing SNMP information on the instance. The instance must be configured with the same community string in order for the SNMP manager to communicate with it. Per SNMP convention, the default community string is &quot;public&quot;, but this should be changed to make the SNMP information more secure.</td>
</tr>
<tr>
<td>Security User</td>
<td>For SNMPv3 only. Specifies the security name required to access a monitored MIB object.</td>
</tr>
</tbody>
</table>
| Authentication Type    | Specifies the authentication protocol. These protocols are used to create unique fixed-sized message digests of a variable length message. Possible values for authentication protocol are:  
  - MD5—Creates a digest of 128 bits (16 bytes).  
  - SHA—Creates a digest of 160 bits (20 bytes).  
  Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet. |
| Authentication Password| For SNMPv3 only. 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 only. Specifies the privacy protocol for the connection between the RealPresence Resource Manager system and the SNMP agent. The RealPresence Access Director system implements communication with authentication and privacy (the authPriv security level as defined in the USM MIB). Possible values for privacy protocol are:  
  - DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet.  
  - AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet. |
| Encryption Password    | For SNMPv3 only. Specifies the password to be associated with privacy protocol. |

---

Polycom, Inc. 517
- 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.

To download the MIB package for a RealPresence Resource Manager system:

1. Go to Admin > Server Settings > SNMP Settings.
2. Click Download MIBs.
3. In the MIBs dialog, select the MIB of interest.
4. Click Download MIB.

Polycom recommends using a MIB browser to explore the RealPresence Resource Manager system MIB. The RealPresence Resource Manager system MIB is self-documenting including information about the purpose of specific traps and inform notifications.

**Polycom RealPresence Resource Manager MIBs**

View the MIBs that the RealPresence Resource Manager system provides for user in monitoring the system.

**Polycom RealPresence Resource Manager-specific MIBs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POLYCOM_BASE-MIB</td>
<td>Includes initialization information for all RealPresence Resource Manager product-specific MIBs. You must load this MIB before POLYCOM-RESOURCE-SCHEDULER-MANAGEMENT</td>
</tr>
<tr>
<td>POLYCOM-RESOURCE-SCHEDULER-MANAGEMENT</td>
<td>RealPresence Resource Manager-specific MIB definition.</td>
</tr>
<tr>
<td>POLYCOM-CMA-MIB</td>
<td>Contains Polycom CMA system legacy traps for backward compatibility. Some traps in this MIB are no longer supported. See the release notes for details on supported traps for this MIB.</td>
</tr>
</tbody>
</table>

**Third-party MIBs adapted for Hardware Monitoring**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adptInfo</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>
</tbody>
</table>

Polycom, Inc. 518
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>dcstorag</td>
<td>Monitoring and information about the hard disks and RAID configuration on the server.</td>
</tr>
<tr>
<td>dellcm</td>
<td></td>
</tr>
<tr>
<td>iDRAC-MIB</td>
<td>Information about iDrac, including data, alerts, and traps</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-ALARM-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>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>
<tr>
<td>SNMPv2-SMI</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>SNMPv2-TC</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
</tbody>
</table>
Configuring Alert Settings

You can configure the RealPresence Resource Manager system to send alerts to users via e-mail for specific types of system and endpoint events.

Setting Up Remote Alerts

The RealPresence Resource Manager system remote alerts functionality is very flexible. It enables 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.

Set Up System Generated E-mail Account

You can set up the e-mail account from which the RealPresence Resource Manager system will send conference notification e-mails and system alerts.

- 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.
- The RealPresence Resource Manager system only sends e-mails for new alerts. The system does not sends e-mails for alert updates.

To set the system generated e-mail account:

1. Go to Admin > Server Settings > E-mail.
2. (Optional) On the E-mail page, select the Allow confirmation e-mails for scheduled conferences check box to activate the e-mail function for conference. With this function enabled, you can enter the text for conference reminder E-mails.
3. In the From Address text box, enter the e-mail account (ASCII only) from which the RealPresence Resource Manager system will send conference notification e-mails and system alerts.
4. In the SMTP Server text box, specify the IP address of the SMTP server from which the RealPresence Resource Manager system will send conference notification e-mails.
5. Click Update.
Enable RealPresence Resource Manager System Remote Alerts

You can enable remote alerts to be sent.

To enable RealPresence Resource Manager system remote alerts:

1. Go to Alert > Remote Alert Setup.
2. Select the check box of Allow remote alert e-mails.
3. Set the Remote Alert delay time after system startup, which is the amount of time (in minutes) that 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 divides alerts into four alert levels: Warning, Minor, Major, and Critical.

By default, most of the Alert Severity Levels are set to Warning for all of the Resource Manager Alert Types they report. You have these options:

- You can leave the Alert Severity Levels set to Warning and create a single remote alert profile that enables you to notify all users assigned that profile about system events of all types.
- You can change some of the Alert Severity Levels to Minor, Major, or Critical 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 Alert > Alert Level Settings.
2. Click the RealPresence Resource Manager tab.
3. Change the alert severity level for the RealPresence Resource Manager alert type system events, as required.
4. Click Update.

Set RealPresence Resource Manager System Alert Threshold Settings

You can view the current default threshold values for RealPresence Resource Manager alarms for each product. When a monitored metric exceeds a threshold, an alarm is raised.
To set the RealPresence Resource Manager Alert Thresholds:

1. Go to Alert > Alert Threshold to display details for each of the installed RealPresence Platform products.
2. Click one of the component types listed on the top of the page. The resources that are available and being monitored for the selected component are displayed.
3. Change applicable fields for each resource on the selected component.
4. Click Update to save the new alarm threshold values.

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 four alert levels: Warning, Minor, Major, and Critical.

By default the Alert Severity Level is set to Warning for all of the Resource Manager Alert Types it reports. You have these options:

- Leave all of the Alert Severity Levels set to Warning and create a remote alert profile for each endpoint type being monitored that enables you to notify all users assigned that profile about all endpoint events applicable to that endpoint type.
- Change some of the Alert Severity Levels to Error and create multiple remote alert profiles that notify different users of endpoint events of different types and severity levels.

To set the endpoint alert level settings:

1. Go to Alert > Alert Level Settings.
2. Click the Endpoints tab.
3. Change the levels for the different types of endpoint events as required.
4. Click Update.

Endpoint Alert Level

Set the levels for the endpoint alert levels.

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Alert indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Control Battery Low Low</td>
<td>The battery in the endpoint's remote needs to be replaced.</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>
</tbody>
</table>
Configuring Alert Settings

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Alert indicates</th>
</tr>
</thead>
<tbody>
<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 dynamically managed endpoint is not registered to the gatekeeper. This alert cannot be used on non-dynamically managed endpoints.</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>
<tr>
<td>Management URL Not Set</td>
<td>The RealPresence Resource Manager system is not one of the management URLs set on the endpoint, possibly because the management URL list is full.</td>
</tr>
<tr>
<td>Touch Control Disconnected</td>
<td>The Touch Control device that was connected to the listed HDX is no longer connected to the HDX.</td>
</tr>
<tr>
<td>Touch Control Software Incompatible with Endpoint</td>
<td>The software version of the Touch Control platform is not compatible with the Endpoint software version.</td>
</tr>
<tr>
<td>SIP URI Not Provisioned</td>
<td>A dynamically managed endpoint at a site with SIP enabled does not have a SIP dial string reservation. The endpoint is provisioned without SIP enabled.</td>
</tr>
<tr>
<td>SIP Status Unknown</td>
<td>The SIP server cannot determine the status of the endpoint.</td>
</tr>
<tr>
<td>SIP Unregistered</td>
<td>The endpoint is not registered with the SIP server.</td>
</tr>
</tbody>
</table>

### Configuring Remote Alert Profiles

Remote alert profiles identify which device alerts are included in alert settings. Note that using a combination of setting alerts by device types, network devices, phones, or endpoints, provides additional granularity in managing device alerts.

**Add a Remote Alert Profile**

You can add a remote alert profile to identify which device alerts from which devices should be included in alert information.
To add a remote alert profile:

1. Go to Alert > Remote Alert Profiles.
3. In the Add Remote Alert Profile dialog, enter Alert Profile Name and Description for the profile.
4. To activate the profile, select 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 Warning, Minor, Major, and Critical.
   - To have a subset of RealPresence Resource Manager system alerts sent as part of this profile, select any combination of Warning, Minor, Major, or Critical. 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 Warning, Minor, Major, and Critical cleared.
6. If you want to request notification trap of endpoints:
   a. Enable the SNMP agent and choose POLYCOMRESOURCE_SCHEDULER_MANAGEMENT for the Supported MIB.
   b. Add an SNMP notification agent.
   c. Select the Send Endpoint Notification Trap check box on the General Info tab of the Add Remote Alert Profile dialog.
7. To use the device type to identify which category of 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.
   - To have all device alerts for all device types sent as part of this profile, in the Device Type Alert Level Mapping page, select Warning, Minor, Major, and Critical for all of the device types.
   - 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 Warning, Minor, Major, or Critical for each device type.
   - 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 Warning, Minor, Major, or Critical 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.
8. To use the device name or the endpoint name to identify which devices and device alerts should be sent as part of this profile, click Alert by Network Device or Alert by Endpoint.
   a. As needed, click Filter to customize the device or endpoint list.
   b. In the Available Devices list, select the devices or endpoints to add to the profile.
   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 Warning, Minor, Major, and Critical 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 Warning, Minor, Major, or Critical 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 *Warning*, *Minor*, *Major*, or *Critical* 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.

The settings are cumulative. If you set device alerts for specific devices, these settings work along with settings made on the *Alert by Device Type* page.

You cannot set the system up to send device alerts for specific desktop video endpoints. Polycom RealPresence Desktop and RealPresence Mobile endpoints are not displayed in the *Available Device* list.

9 To use the endpoint group name to identify which category of devices and device alerts should be sent as part of this profile, click *Alert by Endpoint Group* and configure one of the following:

a As needed, click Filter  to filter the endpoint group list.

b In the *Available Endpoint Group* list, select the endpoint group to add to the profile.

c Click the down arrow to add the devices to the *Monitored Endpoint Group* list and configure one of the following:

♦ To have all device alerts for all devices in the selected endpoint group sent as part of this profile, in the *Monitored Endpoint Group* list, select *Warning*, *Minor*, *Major*, and *Critical* for each endpoint group.

♦ To have a subset of device alerts for all devices in the selected endpoint group sent as part of this profile, for the endpoint groups in the *Monitored Endpoint Group* list, select any combination of *Warning*, *Minor*, *Major*, or *Critical* for each endpoint group.

♦ To have all device alerts for devices in a subset of endpoint groups sent as part of this profile, for each of the endpoint groups in the *Monitored Endpoint Group* list, select *Warning*, *Minor*, *Major*, or *Critical*. Alerts for those endpoint groups in the *Monitored Endpoint Group* list that do not have an alert level selected will not be included.

10 Click OK.

**Related Topics**

Add an SNMP Notification Agent

**Supported Device Types for Remote Alerts**

This section lists all supported device types for which you can set an alert.

**Supported Network Devices**

- RealPresence DMA
- RealPresence Collaboration Server
- RealPresence Access Director
- RealPresence Web Suite Services Portal
- RealPresence Web Suite Experience Portal
- RealPresence Media Suite

**Supported Endpoints**

- V and VSX Series
Associate a Remote Alert Profile With a User

You can associate a remote alert profile with a particular user to track alerts associated with that user.

To associate a remote alert profile with a user:

1. Go to User > Users.
2. To search for a user:
   a. On the Users page, search for the user of interest. Searches for users are not case sensitive.
   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 you want to modify and click Edit.
4. In the Edit User dialog, click Associated Alert Profile.
5. Select the Remote Alert Notification Profile to associate with the user.
6. Click Update.

Edit a Remote Alert Profile

You can edit the settings for a remote alert profile.

To edit a Remote Alert Profile:

1. Go to Alert > Remote Alert Profiles.
2. Select the profile you want to edit and click Edit.

3. As required, edit the General Info, Alert by Device Type, Alert by Network Device, Alert by Endpoint, and Alert by Endpoint Group sections of the Edit Remote Alert Profile dialog.

4. Click OK.

**Disable a Remote Alert Profile**

You can disable a remote alert.

**To disable a Remote Alert Profile:**

1. Go to Alert > Remote Alert Profiles.
2. Select the profile you want to disable and click Edit.
4. Click OK.

**Delete a Remote Alert Profile**

You can delete a remote alert profile when you no longer need it.

**To delete a Remote Alert Profile:**

1. Go to Alert > Remote Alert Profiles.
2. Select the profile you want to delete and click Delete.
   - The profile is deleted from the RealPresence Resource Manager system.

**Disable System Remote Alerts**

You can disable all remote alerts.

**To disable all (system and device) system remote alerts:**

1. Go to Alert > Remote Alert Setup.
3. Click Update.

**Viewing and Deleting Network Device Alerts**

The Alert View page only displays alerts from the following network devices:

- RealPresence DMA
- RealPresence Collaboration Server
- RealPresence Access Director
Configuring Alert Settings

- RealPresence Web Suite Services Portal
- RealPresence Web Suite Experience Portal
- RealPresence Media Suite

The Alert View page does not display the endpoint alerts.

Viewing Alerts

You can view the current state of alarms on the Alert View page. The initial Alert View page shows all alarms.

The alarm colors correspond to the following threshold levels:

- **Gray** System has reached the Warning Value threshold.
- **Yellow** System has reached the Minor Value threshold.
- **Orange** System has reached the Major Value threshold.
- **Red** System has reached the Critical Value threshold.

To view and add comments to active system alerts:

1. Go to Alert > Alert View to display a list of current alerts.
2. Click Filter to filter the alerts by Source IP or Severity.
3. Select an alert.
4. Select View Details at the top to show details about the selected alarms.
5. Select Edit to add comments to a selected alert.

Alert Types

You can set the alert levels for some of the alerts generated by the RealPresence Resource Manager system events form the Alert > Alert Level Settings page.

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Alert indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>BridgeDown (Bridge Down)</td>
<td>A Polycom MCU has failed.</td>
</tr>
<tr>
<td>DatabaseConnectionDown (Database Connection Down)</td>
<td>The connection to the database has been lost.</td>
</tr>
<tr>
<td>LDAPConnectionDown (Enterprise Directory Connection Down)</td>
<td>The connection to the enterprise directory server has been lost.</td>
</tr>
<tr>
<td>LDAPSystemAccountPasswordFail (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>
</tbody>
</table>
### Alert Type

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Alert indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailOverSE200 (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>LicenceCloseToMax (Video License Capacity Threshold Exceeded)</td>
<td>(Non-Clariti Only) The video license threshold, which is set at 95% of capacity, has been exceeded.</td>
</tr>
<tr>
<td>AudioLicencesCloseToMax (Audio License Capacity Threshold Exceeded)</td>
<td>(Non-Clariti Only) The audio license threshold, which is set at 95% of capacity, has been exceeded.</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>LicenseExpiration (License Expiration Warning)</td>
<td>The specified license will expire in less than 30 days.</td>
</tr>
<tr>
<td>LicenseExpired (License Expired Warning)</td>
<td>The specified license has expired or the license cannot be found.</td>
</tr>
<tr>
<td>RedundantServerNotRunning (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>RedundantServerResourceStopped (Redundant Service Stopped)</td>
<td>(In redundant RealPresence Resource Manager system configurations only) The redundancy service has stopped. Contact Polycom Global Support when running into this alert.</td>
</tr>
<tr>
<td>BandwidthUsedSite (Site Bandwidth Threshold Exceeded)</td>
<td>The site bandwidth threshold, which is set at 90% of capacity, has been exceeded.</td>
</tr>
<tr>
<td>BandwidthUsedSubnet (Subnet Bandwidth Threshold Exceeded)</td>
<td>The subnet bandwidth threshold, which is set at 90% of capacity, has been exceeded.</td>
</tr>
<tr>
<td>BandwidthUsedSiteLink (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>CertificateAboutToExpire (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>CertificateExpired (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>DMADown (DMA Down)</td>
<td>The RealPresence DMA system is unreachable.</td>
</tr>
<tr>
<td>E164AliasAssignmentFailed (E164 Alias Assignment Failed)</td>
<td>Auto-assignment of an E.164 alias to a dynamically managed endpoint failed.</td>
</tr>
<tr>
<td>SystemNamingFailed (System Naming Failed)</td>
<td>Auto-assignment of an endpoint name to a dynamically managed endpoint failed.</td>
</tr>
<tr>
<td>DiskSpaceThresholdExceeded (Disk Usage Exceeded)</td>
<td>Disk usage exceeded the configured alert threshold.</td>
</tr>
<tr>
<td>CPUUsageThresholdExceeded (CPU Usage Exceeded)</td>
<td>CPU usage exceeded the configured alert threshold.</td>
</tr>
<tr>
<td>Alert Type</td>
<td>Alert indicates...</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MemoryUsageThresholdExceeded (System Memory Usage Exceeded)</td>
<td>System memory usage exceeded the configured alert threshold.</td>
</tr>
<tr>
<td>ProvisioningCloseToMax (System Capability Settings for Managed Endpoints and Services Number Exceeded)</td>
<td>The number of endpoints exceeds the system capability settings. This alert is only available for the Virtual Edition.</td>
</tr>
<tr>
<td>AutoSystemBackupFTPFailed(Auto system backup failure)</td>
<td>The automatic system backup failed.</td>
</tr>
<tr>
<td>LicenseCloseToMaxNoDMASync (Cannot sync endpoints from DMA because the license threshold has reached)</td>
<td>The system cannot sync endpoints from RealPresence DMA because the license threshold has reached.</td>
</tr>
<tr>
<td>CUCMDown (CUCM Is Unreachable)</td>
<td>The system cannot connect the Cisco Unified Communication Manager server.</td>
</tr>
<tr>
<td>RedundancyDataSyncFailure (Fail to Synchronize Data between Redundant Servers)</td>
<td>(In redundant RealPresence Resource Manager system configurations only) Data replication failed on the redundant servers. You can restart the server and try synchronization again.</td>
</tr>
<tr>
<td>The alert level for the following alerts cannot be changed.</td>
<td></td>
</tr>
<tr>
<td>MonitorServiceStopped</td>
<td>The Monitor Service on redundant server stops running.</td>
</tr>
<tr>
<td>RedundantBothPrimary</td>
<td>Redundant servers have primary licenses</td>
</tr>
<tr>
<td>CDRArchiveFail</td>
<td>The FTP of CDR archive files failed.</td>
</tr>
<tr>
<td>VersionForcedInternal</td>
<td>The RealPresence Resource Manager version is not synchronized with the database version. The system is using the internal database.</td>
</tr>
<tr>
<td>AuditUsageThresholdExceeded</td>
<td>The audit logs exceed the size threshold. The system performs audit log maintenance. The old log files have been deleted.</td>
</tr>
<tr>
<td>IDSDetected</td>
<td>The frequency of network intrusion events has reached or exceeded the threshold. See audit log for details</td>
</tr>
<tr>
<td>DatabaseBackupFailed</td>
<td>Failed to back up the database. See audit log for details</td>
</tr>
<tr>
<td>ConcurrentCallAboutToExceed</td>
<td>The number of the concurrent calls is going to reach the defined threshold.</td>
</tr>
<tr>
<td>ConcurrentCallExceeded</td>
<td>The number of the concurrent calls has exceeded the defined threshold.</td>
</tr>
<tr>
<td>IncompatibleBundle4ep</td>
<td>The endpoint cannot be provisioned with the bundled profile.</td>
</tr>
<tr>
<td>SystemPasswordExpiring</td>
<td>The system credentials have not been changed in (number of days) days. Passwords must be changed in the next (number of days) days.</td>
</tr>
<tr>
<td>SystemPasswordExpired</td>
<td>The system credentials have not been changed in (number of days) days. Passwords should have been changed (number of days) days ago</td>
</tr>
<tr>
<td>Alert Type</td>
<td>Alert indicates...</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>H323IDAssignmentFailed</td>
<td>Failed to assign the H.323 ID to the user.</td>
</tr>
<tr>
<td>SIPURIAssignmentFailed</td>
<td>Failed to generate SIP URI for the user.</td>
</tr>
<tr>
<td>RemoteCDRServerDown</td>
<td>The connection to the remote CDR server is lost.</td>
</tr>
<tr>
<td>LicenseServerDown</td>
<td>The connection to the license server is lost.</td>
</tr>
<tr>
<td>LicenseAcquisitionFailed</td>
<td>Failed to retrieve the system license from the license server.</td>
</tr>
<tr>
<td>TenantE164RangeFull</td>
<td>E.164 number range is already full in Area ((area name)).</td>
</tr>
<tr>
<td>TenantDeviceTypeE164RangeFull</td>
<td>E.164 number range for device type ((device type name)) is already full in Area ((area name)).</td>
</tr>
<tr>
<td>E164RangeFull</td>
<td>E.164 number range is already full.</td>
</tr>
<tr>
<td>DeviceTypeE164RangeFull</td>
<td>E.164 number range for device type ((device type name)) is already full.</td>
</tr>
<tr>
<td>LocalSysLogServerDown</td>
<td>The connection to the local syslog server is lost. The connection can not be recovered automatically.</td>
</tr>
<tr>
<td>MigrateLicenseFeatureAllocationFailure</td>
<td>Failed to migrate license feature allocation.</td>
</tr>
<tr>
<td>MigrateInstanceFailure</td>
<td>Failed to migrate network instances.</td>
</tr>
<tr>
<td>NetworkDeviceIPConfigFailure</td>
<td>Network configuration Failed.</td>
</tr>
<tr>
<td>NetworkDeviceLicenseConfigFailure</td>
<td>License server address provision failed or license refresh failed.</td>
</tr>
<tr>
<td>NetworkDeviceConfigFailure</td>
<td>Failed to add, create or edit the network device.</td>
</tr>
<tr>
<td>GroupSettingNTPFailure</td>
<td>NTP configuration failed.</td>
</tr>
<tr>
<td>GroupSettingADFailure</td>
<td>Enterprise directory configuration failed.</td>
</tr>
<tr>
<td>GroupSettingChangePasswordFailure</td>
<td>Failed to change password.</td>
</tr>
<tr>
<td>GroupSettingSNMPFailure</td>
<td>SNMP configuration failed.</td>
</tr>
<tr>
<td>TotalCPUUsageThreshold</td>
<td>CPU utilization of the system that the network instance (instance name) belongs to has exceeded the CPU usage threshold.</td>
</tr>
<tr>
<td>NetworkInterfaceUsageThreshold</td>
<td>Network interface bandwidth of the system that the network instance (instance name) belongs to has exceeded interface usage threshold.</td>
</tr>
<tr>
<td>StorageDiskUsageThreshold</td>
<td>Disk utilization of the system that the network instance (instance name) belongs to has exceeded the disk usage threshold.</td>
</tr>
<tr>
<td>VideoPortsUsageThreshold</td>
<td>Video port utilization of the system that the network instance (instance name) belongs to has exceeded the video port usage threshold.</td>
</tr>
<tr>
<td>AudioPortsUsageThreshold</td>
<td>Voice port utilization of the system that the network instance (instance name) belongs to has exceeded the audio port usage threshold.</td>
</tr>
</tbody>
</table>
Configuring Alert Settings

Delete Active Alert
You can delete active alarms on the Alert View page.

To delete an active alert:
1. Go to Alert > Alert View to display a list of current alerts.
2. Select an alert you want to delete and click Delete.
3. Click Yes to confirm the deletion.

View Endpoint Event Status
You can monitor endpoint alerts by viewing the endpoint event status. You can also get e-mails when endpoint alerts happen by configuring the remote alert profiles and e-mail address.

To view endpoint event status:
1. Go to Endpoint > Monitor View.
2. View the icons in the Status column:
   - Error: the event status is Error, its corresponding alert level is Critical.
   - Warning: the event status is Warning, its corresponding alert levels are Warning, Minor, or Major.

You can hover your cursor over the icon to see the error message.

Related Topics
Configuring Remote Alert Profiles
Set Up System Generated E-mail Account
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.

Creating System Backups

Polycom recommends configuring automatic system backups to be archived weekly. This archive makes system restoration much simpler. You can configure automatic system backups in addition to being able to download a system backup at any time.

Users assigned the Administrator role can create backups of the existing system. System backups are created in a .zip format which includes both the database backup files and the system settings.

Create an Automatic System Backup

Polycom recommends scheduling regular system backups. When you configure automatic system backups, the system backup zip file is automatically created and sent via FTP site to an external server. Be sure the external storage server has enough space to store regular backups. Verify the size of the backup file occasionally to ensure transfer success.

If you have enabled the RealPresence Resource Manager whitelist, you need to include the IP of the FTP site you use to store system backups in the whitelist.

To schedule automatic system backups:

1. Go to Admin > Maintenance > Backup/Restore System Settings.
2. Configure the settings for FTP of Auto System Backup.
3. To verify that the FTP settings are functional, click Test Archive Settings. If the RealPresence Resource Manager system cannot contact the FTP server, the system generates an alert.
4. When the settings are correct, click Save Settings.

Related Topics

Create a Whitelist to Manage Access
Configuring Alert Settings
FTP of Auto System Backup Settings
FTP of Auto System Backup Settings

Configure the settings for FTP of Auto System Backup.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FTP of Auto System Backup</td>
<td>Select this check box to enable automatic system backups to be sent to an external server via FTP.</td>
</tr>
<tr>
<td>Last Successful Transfer Time</td>
<td>Displays the date and time of the last time a system backup was successfully created and transferred.</td>
</tr>
<tr>
<td>Next Transfer Date</td>
<td>Use the calendar to set up the next transfer date.</td>
</tr>
<tr>
<td>Transfer Start Time</td>
<td>Set the start time of the next transfer and all subsequent transfers. Time format is in 24 hour format. For example, 22:00 is 11 p.m. Do not schedule system backups during peak server hours as it can affect system performance.</td>
</tr>
<tr>
<td>Auto System Backup Transmission Frequency (In Days)</td>
<td>Set the number of days between each transfer.</td>
</tr>
<tr>
<td>Host name or IP Address of FTP server</td>
<td>Specifies the server to which the system backup will be transferred. If you have enabled the RealPresence Resource Managersystem's whitelist, be sure that the IP address of the FTP server is listed on the whitelist.</td>
</tr>
<tr>
<td>FTP Port</td>
<td>Specifies the port through which the system backup will be transferred. By default, the FTP port is 0. 0 stands for auto-detecting well-known FTP port 21 and 990.</td>
</tr>
<tr>
<td>FTP User Name</td>
<td>Specifies a user name and password combination for accessing the FTP server. This must be a valid user account on the FTP server.</td>
</tr>
<tr>
<td>FTP Password</td>
<td></td>
</tr>
<tr>
<td>FTP Directory</td>
<td>Specifies the directory on the server to which the system backup will be transferred. The default directory is the root folder of the FTP server. If you want to use a different directory, you need to create that directory on the FTP server first. For example, create an .AutoBackup folder on the FTP server and then indicate that directory name as the FTP Directory in the RealPresence Resource Manager system.</td>
</tr>
</tbody>
</table>

Create a System Backup Manually

You can manually create a backup archive of a RealPresence Resource Manager system including system configuration settings and database files at any time. You can choose this option even if you have already configured automatic system backups.

When you choose this option, you must download the archive and save it to a location of your choice.

Once the backup archive is downloaded, it can be used to restore the system to its last archived configuration after a disastrous system failure.
System archives do not include system and audit logs. If you want to archive these logs, you must do so separately.

To manually create a system backup:

1. From the RealPresence Resource Manager system web interface, go to Admin > Maintenance > Backup/Restore System Settings.
2. When the Backup/Restore System Settings page appears, click Create and Download a Backup Archive.
3. In the Select location for download dialog, enter a unique File name, browse to a location on your system and click Save.
   A File Download dialog 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.

Related Topics

Managing Audit Log Files

Restoring the System

A user assigned the Administrator role can restore a RealPresence Resource Manager system using a backup archive.

For a-la-carte and Clariti, after restoring the system with a backup archive using off-line license, you must activate the license of the system again.

When you restore databases:

- Do not allow users to connect to the system during the restoration process.
- Restore all of the system databases at the same time.
- Restore all of the system databases from backups that were taken at the same time.
- Restart the system server when the restoration process is finished.

To restore a system from a backup archive:

1. Restore the system to its factory default image.
2. Perform first time setup. For more information about First Time Setup, see the Polycom RealPresence Resource Manager System Getting Started Guide for this release.
3. If using a certificate, re-install the certificate before restoring the backup archive.
   If you had installed a certificate on your system, that certificate is not restored with the system archive. You will need to re-install the certificate on the system before restoring the backup archive.
4. Restore the system 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.

5. Activate and configure license.
   - In off-line mode, license cannot be restored. After restoring the system using the back up file, you will see the License Setup page. You need to import your license file again to activate the license.
   - In on-line mode, if you modify the RealPresence Resource Manager IP address, after restoring the system with Restore Network Settings selected, all the allocated licenses are lost. You need to enable and configure the Polycom license server, and then re-locate the licenses.

6. Upload the endpoint update packages.
   If you have endpoint packages uploaded on the RealPresence Resource Manager system, you need to re-upload the packages for your endpoint updates.

**Related Topics**

- Restore to Factory Default Image
- Restore from a Backup Archive

---

**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. This DVD should have the base image of the RealPresence Resource Manager system server software.

- This is a last resort, so never do this without being instructed to do so by PGS support.
- This process will wipe out your system database and all other system data.
- The Restore to Factory Default DVD is specific to the RealPresence Resource Manager system server type and version.

**Restore from a Backup Archive**

A user with the Administrator role can restore the RealPresence Resource Manager system using a backup archive. You can use 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.

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 > Maintenance > Backup/Restore System Settings.
2. In the Select Archive File section of the Backup/Restore System Settings page, click ...
3. 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 usable 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.
System Maintenance and Troubleshooting

You can troubleshoot problems with RealPresence Resource Manager system logs, Troubleshooting Utilities, and other functions.

System Log Overview

The detailed technical data in the system log files can help Polycom Global Services resolve problems and provide technical support for your system.

In such a situation, your support representative may ask you to download log archives and send them to Polycom Global Services. You may be asked to manually roll logs in order to begin gathering data anew. After a certain amount of the activity of interest, you may be asked to download the active logs and send them to Polycom Global Services.

You can choose to store system logs on your local server in addition to using an external syslog server, according to parameters you choose.

Related Topics

System Management and Maintenance
Available System Logs

The RealPresence Resource Manager system provides the following system logs:

<table>
<thead>
<tr>
<th>System Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jserver</td>
<td>RealPresence Resource Manager system application log. The log file that shows information related to the internal LDAP, SNMP, DM, XMPP, Site Topology and dynamically managed endpoint login and provisioning functionality. <strong>Note:</strong> When you set the logging level to Debug for the Jserver log, you can also use the Activity Filter tab to specify individual IP addresses or users to emphasize in the Jserver log.</td>
</tr>
<tr>
<td>DeviceManager</td>
<td>Log file for the device management process.</td>
</tr>
<tr>
<td>Conference</td>
<td>Conference scheduling log used by the conference scheduling process. This log contains debug information on how a conference is created.</td>
</tr>
<tr>
<td>Corosync</td>
<td>Redundancy log that records redundancy status and activity such as corosync, pacemakers, dataeng, lrmd and so on.</td>
</tr>
<tr>
<td>Redundancy</td>
<td>Redundancy log that record related information once a failover has occurred.</td>
</tr>
<tr>
<td>AudioPhone</td>
<td>Real-time phone management log that records file requests and responses to phones, notification events from phones at the debug level, and phone sync information between the RealPresence Resource Manager system and CUCM.</td>
</tr>
</tbody>
</table>

Related Topics

Customize Jserver Log to Target Specific Activity

Managing Locally Stored System Logs

When you choose to store system logs on the local RealPresence Resource Manager system, you can easily download them directly from the system, customize the logging settings, as well as determine how often the logs are restarted (rolled).

View Locally Stored System Log Files

Many of the RealPresence Resource Manager system components can write a System Log File when they experience an error or issue.

Audio phone logs can only be viewed and downloaded from the Endpoint > Monitor View page.

To view or download system log files:

1. Go to Admin > Maintenance > System Log Files.
   - The System Log Files list appears listing the logs for the given time period.
2. Select the log file you want to view and click Download.

Polycom, Inc.
Change Logging Level for Locally Stored Logs

You can configure the local log level for the following system logs:

- Jserver
- DeviceManager
- Conference
- Corosync
- Redundancy
- AudioPhone

To edit the current system log level for local logs:

1. Go to Admin > Maintenance > Log Settings.
2. The System Log Files list appears.
3. Select log you want to change.
4. Click Edit.
5. In the Configuration dialog, click Local Settings.
6. Configure the following settings for the specified file. If you set the local level to None, no log file will be stored.
7. Click OK.

Local Settings of Log Files

The table describes the available settings of a log file.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Level</td>
<td>Sets the logging level for the system log file stored on the local server.</td>
</tr>
<tr>
<td></td>
<td>Logging levels include:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Emergency</td>
</tr>
<tr>
<td></td>
<td>• Alert</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Notice</td>
</tr>
<tr>
<td></td>
<td>• Information</td>
</tr>
<tr>
<td></td>
<td>• Debug</td>
</tr>
<tr>
<td>Note:</td>
<td>When you set the logging level to Debug for the JServer log, you can also</td>
</tr>
<tr>
<td></td>
<td>use the Activity Filter tab to specify individual IP addresses or users to</td>
</tr>
<tr>
<td></td>
<td>emphasize in the JServer log.</td>
</tr>
<tr>
<td>Rotation Size</td>
<td>Configures the maximum size the log file can reach before it is rolled.</td>
</tr>
</tbody>
</table>
System Maintenance and Troubleshooting

Download Locally Stored Log Files

You can download a .gz 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 the operating system.

To download the system logs:

1. Go to Admin > Maintenance > System Log Files.
2. Click Download All.
3. To open the .gz file, in the File Download dialog, click Open with, and browse to the program you use to open .zip files.
4. To save the .gz file to your local computer, in the File Download dialog, click Save.

Roll Locally Stored Log Files

You can use the Roll Log action to close and archive locally stored log files and start new log files. Although you can configure an automatic window in which logs are rolled (restarted), you can also manually roll the logs whenever you need to troubleshoot a particular incident.

When you roll locally-stored logs, the following subset of locally-stored logs are archived and restarted.

- Jserver
- DeviceManager
- Conference
- Corosync
- Redundancy
- AudioPhone

To roll the system logs:

1. Go to Admin > Maintenance > System Log Files.
2. Click Roll Logs .
   A message displays confirming the operation and detailing which logs were rolled.
3. Click Close to close the information dialog.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured File Count</td>
<td>Configures the maximum number of this type of log file that can be stored on the local server.</td>
</tr>
<tr>
<td>Rolling Frequency</td>
<td>Configures how often the log file is rolled. When a log file is rolled, a new log file is started and the previous log file is archived on the local server.</td>
</tr>
</tbody>
</table>
**Customize Jserver Log to Target Specific Activity**

You can customize the JServer log to target specific IP or user activity. This can help when troubleshooting issues that may be related to a certain system or user configuration. When you customize the JServer log, you set its logging level to debug and then add up to five Activity Filters that will be displayed in the log. This is usually done in conjunction with rolling the log file to get more targeted results.

**To customize the Jserver log when debugging:**

1. Go to Admin > Maintenance > Log Settings.
   The System Log Files list appears.
2. Select the Jserver log.
3. Click Edit.
4. In the Configuration dialog, click Local Settings.
5. In Local Settings section, select Debug from the Local Level drop-down field.
6. In the Configuration dialog, click Activity Filter Settings.
7. Configure up to five Activity Filters for the log.
   a. Select User or IP from the drop-down box.
      b. Enter the IP address or user you want to view in the log.
         For users, enter the domain and user name, such as `local\admin`.
         For IP addresses, enter a valid IP address, such as `10.34.12.10`.
8. Click OK.

**Managing System Logs using a Syslog Server**

If your IT environment includes an external syslog server, you can choose to have system logs automatically sent to that server to be stored and managed externally from the RealPresence Resource Manager system.

**Store System Logs on a Remote Syslog Server**

You can select individual logs and choose to have them stored on a remote syslog server. Logs can be stored both locally and on a syslog server at the same time. You can use both methods if you want to customize log settings.

The `corosync.log` and `redundancy.log` include database information that cannot be completely stored on a remote syslog server. Please defer to locally stored files for complete information about redundancy issues.

The `OS-audit` and `OS-secure` logs can only be sorted on a remote syslog server.

**To configure a system log to be sent to a remote syslog server:**

1. Go to Admin > Maintenance > Log Settings.
2. The System Log Files list appears.
3 Select log you want to change.
4 Click **Edit**.
5 In the **Configuration** dialog, click **Remote Settings**.
6 Click **Add** to add a remote log.
7 Configure the following settings for the specified file. If you set the **Remote Level** to **None**, no log file will be stored.
8 Click **OK** to add the remote setting to the list.
9 Optionally, select the remote logs and click **More > Test Remote Connection** to verify that your remote syslog server setting was entered correctly.
10 Click **OK** to exit the dialog.

**Remote Settings of Log Files**

The table describes the available remote settings of a log file.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Level</td>
<td>Sets the logging level for the system log file stored on the local server.</td>
</tr>
<tr>
<td></td>
<td>Logging levels include:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Emergency</td>
</tr>
<tr>
<td></td>
<td>• Alert</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td>• Notice</td>
</tr>
<tr>
<td></td>
<td>• Information</td>
</tr>
<tr>
<td></td>
<td>• Debug</td>
</tr>
<tr>
<td>Remote Host</td>
<td>Indicates the IP address of the remote syslog server.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Indicates the port used to access the remote syslog server.</td>
</tr>
<tr>
<td>Remote Protocol</td>
<td>Indicates the transfer protocol to use. You can select TLS, TCP or UDP.</td>
</tr>
</tbody>
</table>

**Delete a Log from Being Stored on a Remote Syslog Server**

When you delete the remote settings for a system log, it is no longer sent to the syslog server for storage.

To undo remote storage of a system log:

1. Go to **Admin > Maintenance > Log Settings**.
2. The **System Log Files** list appears.
3. Select log you want to modify.
4. Click **Edit**.
5 In the **Configuration** dialog, click **Remote Settings**.

6 Select the remote server settings that you want to delete and click **Delete** 🗑️.
Managing Audit Log Files

Audit logs provide a way to monitor the system for security and system access activity. 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>localhost_access.log</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>kernel.log</td>
<td>Logs are useful not only for understanding the internal operation of a system but also the timing and relationships of activities within the system through the time-ordered messages within a time-stamped log.</td>
</tr>
<tr>
<td>hids.log</td>
<td>Log file that captures intrusion detection alerts.</td>
</tr>
</tbody>
</table>

**Related Topics**

Auditor Responsibilities.

**View and Download Audit Logs**

You can view and download audit log files.

**To view and download audit log files:**

1. Go to Admin > Maintenance > Audit Log Files.
   - The Audit Log Files page appears listing the logs being stored on the system.
2. Select the audit log you want to download and click Download  
3. In the File Download dialog, click **Open** to view the file or click **Save** to save the log file to your local system.
Change Audit Log Settings

Audit logs are automatically kept and stored until the maximum storage amount is of 2 GB is reached. You can configure alerts to be sent when the audit logs reach a specified percentage of the maximum storage available.

Audit logs are automatically rolled, archived, and the oldest logs deleted when the 90 percent of the storage (1.8 GB) is used. An alert is sent to the alert email address you have configured.

To set an alert for audit log storage

1. Navigate to **Admin > Audit Log Files**.
2. Click **Change Settings**.
3. In the **Audit Log File Setting** dialog, configure the percentage of file size usage you want to reach before being alerted. You can set a percentage between 40 and 80 percent of the maximum storage amount of 2 GB.
4. Click **OK**.

Roll Audit Logs

You can archive logs and restart them at any time. This process is called rolling. When you roll audit logs, each existing log is zipped and stored as a .gz file that can be backed up and deleted from the system.

Audit logs are automatically rolled, archived, and the oldest logs deleted when the 90 percent of the storage (1.8 GB) is used. An alert is sent to the alert email address you have configured.

Current logs maintain an extension of .log while archived logs are stored as .gz files.

To roll audit logs:

1. Navigate to **Admin > Audit Logs**.
2. Click **Roll Logs**.
   
   A message dialog informs you that the audit log files were successfully rolled.
3. Click **Close** to close the information dialog.

Backup and Delete Audit Files

The RealPresence Resource Manager system enables you to store audit logs locally until the maximum file storage limit of 2 GB is met. You should periodically roll the logs, and then backup the archived files and delete them from the local system.

You can create a backup of audit files and then delete the files from the server. After you create a backup (a zip file) you are prompted to verify that the files are authentically from the server from which they were downloaded and have not been modified since being downloaded. You need to verify the zip file with the Polycom Verification Utility which is provided.

You must have the auditor role in order to download and delete audit log files.
To backup and delete audit files:

1. Navigate to Admin > Maintenance > Audit Log Files.
2. Select the audit log file(s) that you want to backup and delete.
3. Click Backup and Delete.
4. The files will be saved in your browser’s download folder.
5. In the Backup and Delete dialog, ensure that each audit log file that you want to backup is selected. All audit logs are selected by default, you can deselect the files that you do not want to include in the archive.
6. Click Download Verification Utility if you want to delete the backed-up logs.
   The Polycom File Verification Utility generates a checksum number that can be used as a verification code to ensure that the audit log files have not been modified after they were downloaded.
7. Execute the File Verification Utility and browse to the location of the audit file backup. After doing so, the File Verification Utility will output a value that can be copied to the clipboard.
8. Copy the Verification Value and enter it into the Verification Code section of the RealPresence Resource Manager system dialog.
9. Click Verify and Delete.
   The audit logs are deleted from the RealPresence Resource Manager system.

View RealPresence Resource Manager System Report

The RealPresence Resource Manager System Report can be a useful report. It produces a SystemInfo.txt file that describes the system configuration.

To view the RealPresence Resource Manager System Report:

1. Go to Admin > Maintenance > Troubleshooting Utilities.
2. Click Resource Manager System Report to download the system report.
3. When the File Download dialog appears, either Open or Save the SystemInfo.txt file:
   The report includes this information.

   RESOURCE MANAGER VERSION
   Software version : 8.1.0.0_12-135102
   Hardware version : UNKNOWN
   LDAP Integration : false

   SECURITY SETTINGS
   System under Secure Mode: false

   NETWORK CONFIGURATION
   System name : XMA-114
   System DSCP tag : 0
System IPv4 Address : 10.220.202.114
System IPv6 Address : N/A
System IPv6 Link local: N/A
System subnet mask : 255.255.255.0
System default gateway: 10.220.202.254
System DNS domain : pct-cmaqa.com
System DNS server 1: 172.21.120.179
System DNS server 2: N/A

LICENSE INFO
Total number of licenses : 100
Number of licenses in used: 0

CONFERENCE SETTINGS
Conference Time Warning : true
Include Conference Owner in new Conference: false
Allow Overbooking of dial-In participants : false
Conference PIN Length : 6

SESSION MANAGEMENT SETTINGS
Remote Access Connection is allowed : true
Resource Manager User Interface timeout (in sec): 0
Max number of sessions per user : 5
Max number of sessions per user enabled : false
Max number of sessions per system : 50

LOCAL USER ACCOUNT CONFIGURATION
Failed login threshold : 3
Failed login windows (hours) : 1
Lockout duration (minutes) : Indefinite
Account Inactivity threshold (days): -1

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 Settings: N/A
- Cipher Suite: STANDARD_MODE
- Allow Server Self Signed Cert: true
- Require Clients Send Certificate: false
- External Server Settings: N/A
- Trust Server Self Signed Certificate: false
- Validate Server's hostname: false
- Validate Server's Date Range: false
- Validate Server's Revocation: false
- External Client Settings: N/A
- Trust Client Self Signed Certificate: false
- Validate Client's Date Range: false
- Validate Client's Revocation: false
- Certificate Common Name: Resource Manager Self-Signed Certificate
- Certificate Alias: 1
- Certificate Issuer: Resource Manager Self-Signed Certificate
- Certificate Common Name: XMA-114.pct-cmaqa.com
- Certificate Alias: default
- Certificate Issuer: XMA-114.pct-cmaqa.com

REDUNDANCY INFORMATION
- Server 1 IP address: N/A
- Server 1 is Active: false
- Server 1 is ON: false
- Server 2 IP address: N/A
- Server 2 is Backup: true
- Server 2 is ON: false
- Virtual IP address: N/A

DATABASE CONFIGURATION
- Use external DB: false

**Troubleshooting Utilities**

The RealPresence Resource Manager system has a **Troubleshooting Utilities** panel 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. You also can restart and shutdown your system from here.

The diagnostic files include:

- **Restart/Shutdown**: Click the buttons to restart or shut down the RealPresence Resource Manager system.
● **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,

● **Resource Manager System Report**: Use this option to generate and download a `SystemInfo.txt` file that describes the system configuration.

● **Test Network Connection**: Use this option to perform a **Traceroute** or **Ping** operation. **Traceroute** enables you to investigate the route path and transit times of packets as they travel across an IP network. **Ping** enables you to test the availability of a host on an IP network.

● **View Phone Management Log**: Use this option to troubleshoot phone management issues by checking the phone management real-time log:
  - File requests and responses to phones: phone’s MAC address, file name, success or fail response in info level.
  - Notification event from phones at debug level.
  - Phone sync information between the RealPresence Resource Manager system and CUCM, such as the MAC address read from CUCM API and the failure reason when phones fail to be added in info level.

### Capture a Trace Using Filters

When capturing a trace, you can filter to make the capture more accurate. You can use any filters that `tcpdump` command supports. For example, use the `tcp port 22` filter for catching SSH communication.

To capture a trace:

1. Go to **Admin > Maintenance > Troubleshooting Utilities**.
2. Enter a filter.
3. Click **Start Capture**.
   
   You can view the trace file at **Admin > Maintenance > System Log Files**.

### Working with Phone Management Log

You can view, search text in, or download the real-time phone log. You can also pause or resume the logging process, clear the log window, or change the settings of the log.

### View Phone Management Log

You can troubleshoot phone management issues by viewing the real-time phone log.

To view the real-time phone log:

1. Go to **Admin > Maintenance > Troubleshooting Utilities**.
2. Click **View Phone Management Log**.
3 Click Pause to pause or click Resume to resume the logging process.

**Filter Phone Management Log**

You can locate specific errors or phones in the real-time phone log by search.

**To search in the real-time phone log:**

1. Go to Admin > Maintenance > Troubleshooting Utilities.
2. Click View Phone Management Log.
3. In the View Real-time Phone Log window, enter your keywords in the top right text box and press Enter.
4. To remove the filter or clear the search result, delete your keywords and press Enter.

**Download Phone Management Log**

You can download the real-time phone log to your local drive for reference.

**To download the real-time phone log:**

1. Go to Admin > Maintenance > Troubleshooting Utilities.
2. Click View Phone Management Log.
3. In the View Real-time Phone Log window, click Download to download the log.
   - If you download after filtering the log, the downloaded log still contains the full log instead of the filtered contents.

**Clear Phone Management Window**

You can clear the real-time phone log window to get the log from the current point. By default the window shows the latest 1000 lines in the log. If there’s no updates in the log after you clear the window, the window still shows the previous contents.

**To clear the real-time phone log window:**

1. Go to Admin > Maintenance > Troubleshooting Utilities.
2. Click View Phone Management Log.
3. In the View Real-time Phone Log window, click Clear to clear the window.
   - If you download the log after clearing the window, the downloaded log still contains the full log.

**Troubleshooting Specific Types of Issues**

This section describes information on troubleshooting specific types of issues on the RealPresence Resource Manager system.
**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 Network 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 RealPresence Resource Manager system is restarted, some registrants that were previously online are now offline.</td>
<td>• Some endpoints do not re-register when the RealPresence Resource Manager system goes down. • Some MCUs do not re-register 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 Network 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. |
Diagnostics for your Dell Server

If your RealPresence Resource Manager system is shipped with a Dell D620 server, you need to have a USB keyboard and a monitor in order to run diagnostics.

Perform these diagnostics only under the guidance of Polycom Global Services.
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.

Without specific notification, the ports listed in this section are not configurable.

Open Inbound Ports on the RealPresence Resource Manager System

This table lists the open inbound ports on the RealPresence Resource Manager system and provides a description of their use.

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 22</td>
<td>SSH port for remote access.</td>
</tr>
<tr>
<td>TCP/UDP 53</td>
<td>DNS port. Used to support Geographical redundancy. Blocked in single server deployment (no redundancy).</td>
</tr>
</tbody>
</table>
| TCP 80        | • HTTP web server, through which the web application displays and where Polycom endpoints post status messages.  
                  • HTTP web access for GUI.                                              |
| TCP/UDP 161 or TCP 8161 | SNMP listener  
                          You can configure to use 161 or 8161 from the GUI.                  |
| TCP 389       | Directory services (LDAP)                                                    |
| TCP 443       | HTTPS (TLS) web server listener. Used to provide web access for endpoints. Used to provision endpoints and communicate with the Polycom RealPresence Collaboration Server (RMX) and the Polycom RealPresence DMA system. |
| TCP 445       | Active Directory single sign-on and RealPresence Resource Manager user account management. |
| TCP 3601      | (Polycom proprietary service) Global Address Book listener with which endpoints register |
# 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 3333/9333</td>
<td>License related communication.</td>
</tr>
<tr>
<td>TCP 4449</td>
<td>(Polycom proprietary service) TLS/OpenDS (Data store for site topology) admin port. Open only when RealPresence Resource Manager system is integrated with a RealPresence DMA system. Blocked if no RealPresence DMA is integrated.</td>
</tr>
<tr>
<td>TCP 5405</td>
<td>Used for redundancy services (corosync, pacemaker). Blocked in a single server environment.</td>
</tr>
<tr>
<td>TCP 5222</td>
<td>Presence service (XMPP)</td>
</tr>
<tr>
<td>TCP 8443/443</td>
<td>HTTPS (TLS) web access for GUI and REST API.</td>
</tr>
<tr>
<td>TCP 80</td>
<td>HTTP web access for GUI.</td>
</tr>
<tr>
<td>TCP 8989</td>
<td>HTTP web access to display upgrade log in user’s browser during system upgrade. The port is disabled for all normal operations except upgrade. The RealPresence Resource Manager system’s upgrade process automatically enables it when upgrade starts, and disables it when upgrade finishes.</td>
</tr>
<tr>
<td>TCP 60000 - 61000</td>
<td>FTP data port. Used with you integrate a Cisco Unified Communications Manager system with a RealPresence Resource Manager system. An FTPDATA port is allocated when a Polycom phone is provisioned and needs to download files from the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>TCP 20</td>
<td>Used to FTP data to endpoints</td>
</tr>
<tr>
<td>TCP 21</td>
<td>Used to access the telnet interfaces on endpoints</td>
</tr>
<tr>
<td>TCP/UDP 23</td>
<td>Used to access the telnet interfaces on endpoints</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 email messages to SMTP servers</td>
</tr>
<tr>
<td>TCP/UDP 53</td>
<td>Used to access domain name servers (DNS)</td>
</tr>
<tr>
<td>UDP 67</td>
<td>Used to access DHCP server.</td>
</tr>
<tr>
<td>UDP 68</td>
<td>Used to access DHCP server.</td>
</tr>
<tr>
<td>TCP 80</td>
<td>Used to access the web application on endpoints.</td>
</tr>
<tr>
<td>TCP 8080</td>
<td>Used to access the web application on MCUs.</td>
</tr>
<tr>
<td>UDP 123</td>
<td>Used to access NTP server.</td>
</tr>
</tbody>
</table>
System Security and Port Usage

Internal Ports used by the System

The following ports are used internally by the RealPresence Resource Manager system. They are not exposed (via firewall) and cannot be accessed by other servers.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 1161</td>
<td>SNMP service.</td>
</tr>
<tr>
<td>TCP 5432</td>
<td>PostgreSQL</td>
</tr>
<tr>
<td>TCP 6389</td>
<td>OpenDS port. Used for site topology management.</td>
</tr>
<tr>
<td>TCP 9443</td>
<td>Used to communicate via JServer and Netty.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 161</td>
<td>SNMP query</td>
</tr>
<tr>
<td>TCP/UDP 162</td>
<td>Used to access SNMP.</td>
</tr>
<tr>
<td>TCP/UDP 389</td>
<td>Used to access directory (LDAP) services</td>
</tr>
</tbody>
</table>
| TCP 443       | • Secure access to endpoint devices (SSL) including Polycom CMA Desktop.  
                  ▲ Source port: 32768-61000  
                  ▲ Destination IP/port (FQDN domain): polycom.flexnetoperations.com  
| TCP 445       | Active Directory Single Sign-on                  |
| TCP/UDP 636   | Used to access LDAP over TLS/SSL (LDAPS)         |
| TCP/UDP 3268  | Used to access the Microsoft Active Directory Global Catalog using StartTLS |
| TCP/UDP 3269  | Used to access the Microsoft Active Directory Global Catalog using LDAP-S |
| TCP 443/8443  | API communications                               |
| TCP 5060      | Used to send check sync messages to phones.      |
| ICMP Type: 8, Code: 0 | Ping to detect status of network instances. |
Working in a vCenter Environment

In a vCenter environment, the RealPresence Resource Manager system can also (with the proper permissions) create, deploy, and manage virtual instances of RealPresence Platform products. This versatility enables an administrator to manage all Polycom RealPresence products from RealPresence Resource Manager. There is no need to go to the vCenter user interface to manage RealPresence Clariti products.

Basic Configuration Setup

In a vCenter environment, basic configuration includes adding a provider and a resource group. This section covers how to manage providers and resource groups.

Managing Providers

In a vCenter environment, a provider record specifies the information required to access a vCenter Server, enabling the RealPresence Resource Manager system to use the vCenter APIs to create, manage, and monitor virtual RealPresence instances. The RealPresence Resource Manager environment must have a provider record for each vCenter Server to which it must connect.

Add a Provider

The provider information includes the URL for the VMware vCenter Server and user account credentials required to create new instances and manage existing ones.

To add a provider:

1. Log into the RealPresence Resource Manager system as a user with Admin privileges.
2. Go to Network Device > Providers and click Add .
3. In the Add Provider page, enter the provider details.
4. Click OK to add the provider.

Add Provider Settings

The table describes the available settings when you add a provider.
Working in a vCenter Environment

Edit a Provider
From the Providers page, you can select a provider to edit.

To edit a provider:
1. Go to Network Device > Providers.
2. Select the provider you want to edit and click Edit.
3. Edit the provider information.
4. Click OK to save the changes.

Delete a Provider
You can delete a provider when it is no longer applicable to your RealPresence Resource Manager configuration. A RealPresence Resource Managersystem within a vCenter environment requires at least one provider.

To delete a provider:
» Select the provider you want to delete and click Delete, and follow the instructions in the confirmation dialog.

Managing Resource Groups
Resource groups are required only in vCenter environments. They provide a way to logically group and effectively manage the available resources.

For example, you may want to deploy compute-intensive and memory-intensive instances on specific clusters or hosts in your vCenter that have ample capacity. You can create one or more resource groups that contain those resources and then monitor them separately to ensure appropriate capacity and performance.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Name</td>
<td>A unique name (80 characters maximum) for the provider.</td>
</tr>
<tr>
<td>Provider Type</td>
<td>VMware is the only selection available.</td>
</tr>
<tr>
<td>URL</td>
<td>The URL for the VMware vCenter Server. The syntax for a VMware provider URL is: https://&lt;vCenter IP address&gt;/sdk In place of the IP address, you can use the fully qualified domain name (FQDN) for the vCenter.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user ID for accessing the VMware vCenter. See Appendix 1: Required vCenter Permissions in the Getting Started Guide for a detailed description of the vCenter permissions required to enable various RealPresence Resource Manager capabilities.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user.</td>
</tr>
</tbody>
</table>
Add a Resource Group to a Provider

A resource group operates within a provider in a RealPresence Resource Manager system. You can add a resource group to any defined provider.

To add a resource group to a provider:

1. Go to Network Device > Providers.
2. Select the provider you want to add the resource group.
4. Enter a unique Name.
5. Select a Data Center, Host/Cluster, and optional Resource Pool from the lists of those available.
6. If the data center has folders, and you want to deploy new virtual instances to a folder, enter the folder path in the Inventory Sub Path field.
   The system appends what you enter to the end of the Inventory Full Path entry, which initially contains the name of the data center, followed by /vm. New virtual instances are deployed to the last folder in the full path.
7. Click the Storage Resource tab.
8. In the Available section, select the storage resource(s) and click the arrow icon to move the list to the Selected section.
9. Click the Network Resource tab.
10. In the Available section, select the network resource(s) and click the arrow icon to move the list to the Selected section.
11. Click OK to add the new resource group to the system.

With a provider and resource group in place, you can begin adding other RealPresence Virtual Edition products to your vCenter environment.

Edit a Resource Group

As your organization’s capacity needs grow, or when you need to take a host out of service for maintenance, you may need to add or remove resources from a defined resource group.

To edit a resource group:

1. Go to Network Device > Providers.
2. Select the appropriate provider, click Folder ahead of the selected provider to expend the folder, you will see the resource group added on this provider.
3. Select the resource group.
4. Click Edit to open the Edit Resource Group dialog.
5. Edit the settings as needed.
6. Click OK to save the changes.
Delete a Resource Group

You can delete a resource group that is no longer relevant to your RealPresence Resource Manager system. A resource group can be deleted only if it contains no instances.

To delete a resource group:
1. Go to Network Device > Providers.
2. Select the appropriate provider, click Folder ahead of the selected provider to expend the folder, you will see the resource group added on this provider.
3. Select the resource group that you want to delete and click Delete.
4. Click OK to delete the selected resource group.

Instance Management

In a vCenter environment where the RealPresence Resource Manager system has the appropriate write permissions, you can use the RealPresence Resource Manager system to create a new instance. In this case, the RealPresence Resource Manager system will do license management by default.

When you create an instance of a RealPresence Resource Manager component, you configure the network settings for the instance, including the IP address, subnet mask, and gateway to allow users to access the instance on your network. You can also choose to assign those network settings using DHCP.

To add a virtual instance:
1. Go to Network Device > Instances.
2. Click Add.
3. Select a device type that you want to add.
4. Select Provider from the Add By drop-down list.
5. Do one of the following:
   - Select New to add a new instance and specify the parameters.
   - Select Existing to add an existing instance and specify the parameters.
6. Click OK to add this instance.

Adding a New Virtual Instance

The table describes the available settings when you add a new virtual instance.
Adding an Existing Virtual Instance

<table>
<thead>
<tr>
<th>Field</th>
<th>Value/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the selected instance. After you select an existing instance from the Instance drop-down list, this field will be populated automatically.</td>
</tr>
<tr>
<td>Version</td>
<td>Enter the version number of the instance.</td>
</tr>
<tr>
<td>Admin User</td>
<td>Enter the administrator user name with which the RealPresence Resource Manager system can log into the instance.</td>
</tr>
<tr>
<td>Admin Password</td>
<td>Enter the password for the administrator user. The credentials must be correct in order for the RealPresence Resource Manager system to manage the instance.</td>
</tr>
<tr>
<td>Provider</td>
<td>Select the provider that manages the instance being added.</td>
</tr>
<tr>
<td>Data Center</td>
<td>Select the data center in which the instance is deployed.</td>
</tr>
<tr>
<td>Host / Cluster</td>
<td>Select the host or cluster in which the instance is deployed.</td>
</tr>
<tr>
<td>Resource Pool</td>
<td>If the selected host or cluster contains resource pools, select the pool in which the instance is deployed.</td>
</tr>
<tr>
<td>Instance</td>
<td>Select the instance from the list of instances in the location you specified.</td>
</tr>
</tbody>
</table>
To edit an virtual instance:

1. Go to Network Device > Instances.
2. Select an instance that you want to edit and click Edit.
3. Edit the instance settings as needed.

To delete an virtual instance:

1. Go to Network Device > Instances.
2. Select an instance that you want to delete and click Delete.
3. Click OK to confirm the deletion.

Delete Uploaded Images

The system only reserves 8 GB for saving images. If the uploaded images are over 8 GB, you cannot upload any image with the Fail to create an OVF file, check your disk space and re-upload the file error. In this case, you need to delete the unused images.

To delete an image:

» Click Delete beside the uploaded images in the Image drop-down list when adding or editing an instance add by provider.

Service Integration

You can enable service integration in a vCenter environment. The configuration is same as in non-vCenter environment. When adding a new instance by a provider, you need to enable service integration after the new instance is added.

vCenter Permissions

In a vCenter environment, you can use the RealPresence Resource Manager system to deploy virtual editions of Polycom products.

The purpose of this appendix is to define a minimum set of permissions that RealPresence Resource Manager requires for basic user workflows related to adding and monitoring virtual machine (VM) instances.

For a more complete description of the roles and permissions available in vCenter, refer to the documentation for VMware vSphere. The permissions described here can be applied from the vCenter level down to the individual host or cluster level.

VMware APIs Used by RealPresence Resource Manager

RealPresence RealPresence Resource Manager uses a relatively small number of the APIs exposed by VMware. In general, the API usage relates to:
● Determining vCenter organization (data centers, hosts/clusters, network, and disk storage)
● Manipulating VMs (deployment, power on and off, and deletion)
● Monitoring RealPresence Resource Manager-managed resources within vCenter

RealPresence Resource Manager does not affect the vCenter organization at any level higher than the VMs themselves. In this sense, the permissions required by RealPresence Resource Manager are minor compared with the total number of permissions available in vCenter.

Since most APIs only require read-only access to vCenter by RealPresence Resource Manager, the rest of this appendix focuses on the features in RealPresence Resource Manager that require write access to vCenter.

### Instance Management

Monitoring and managing instances is primarily a read-only operation with respect to vCenter, with a few exceptions. The current state data for VMs is gathered through an API that allows RealPresence Resource Manager to access current details of the VM itself. Parameters such as the state (on or off) of the VM, the state of the Guest OS Tools (running or not), and various other parameters are required by RealPresence Resource Manager to reflect the current state of Polycom product VMs and notify an administrator of potential issues.

Instance management also includes write-access actions such as the ability to power on, power off, or delete an individual VM. Permissions required to perform these actions are listed in the following table.

Permissions are listed in the hierarchy in which they are specified in the vSphere client. Please see vSphere client documentation for further details.

#### Privileges Required for Managing a VMware Instance

<table>
<thead>
<tr>
<th>Entity</th>
<th>Category</th>
<th>Privilege required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions</td>
<td>N/A</td>
<td>Validate session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View and stop sessions</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Interaction</td>
<td>Power off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power on</td>
</tr>
<tr>
<td>Inventory</td>
<td></td>
<td>Remove</td>
</tr>
</tbody>
</table>

### Two Methods for Adding VM Instances in a vCenter

The two methods for adding a VM instance to RealPresence Resource Manager system in a vCenter are:

- Create the VM using RealPresence Resource Manager.
- Allow RealPresence Resource Manager to scan the vCenter infrastructure to find and add an existing VM instance.

The first method enables RealPresence Resource Manager to deploy an instance of a Polycom product to a specific Resource Group.¹

---

¹ “Resource Group” is a RealPresence Resource Manager abstraction representing the physical location of a VM within a vCenter by specifying the data center, host or cluster, network, and disk resources.
In both cases, after a VM has been added, RealPresence Resource Manager monitors several “health” parameters-including CPU, memory and disk usage—for the Resource Group that contains the instance, and can generate alarms based on thresholds that are set for each of those operating parameters.

Note that VM instances are not monitored individually using VMware APIs. Instead, instance monitoring, or, more appropriately, application monitoring, uses the built-in SNMP infrastructure that exists in most Polycom products.

**Creating an Instance**

Instance creation, or deployment, is a process in which RealPresence Resource Manager dynamically creates an instance based on a Polycom product’s OVA image. Creating an instance requires several permissions related to the allocation of resources within vCenter. The following table lists the unique permissions required for this operation.

Permissions are listed in the hierarchy specified in the vSphere client. Please see vSphere client documentation for further details. Also, note that these are the specific permissions required for creating an instance and should be merged with the permissions for managing an instance.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Category</th>
<th>Privilege required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore</td>
<td>N/A</td>
<td>Allocate space</td>
</tr>
<tr>
<td>Global</td>
<td>N/A</td>
<td>Act as vCenter Server</td>
</tr>
<tr>
<td>Network</td>
<td>N/A</td>
<td>Assign network</td>
</tr>
<tr>
<td>vApp</td>
<td>N/A</td>
<td>Import</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>Configuration</td>
<td>Add new disk Advanced</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Operation Program Execution</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Operation Queries</td>
</tr>
</tbody>
</table>

**Monitoring vCenter Resources**

Regardless of the method used to add a VM to RealPresence Resource Manager in a vCenter, a Provider and Resource Group will exist, defining the location for each VM within RealPresence Resource Manager. For these entities, monitoring involves polling vCenter APIs to determine whether there are connectivity issues or whether thresholds have been exceeded; alarms are raised in both cases. The same data is also stored for retrieval at a later time.

---

1. An OVA is a compressed archive of the Open Virtualization Format (OVF). OVA is the format in which Polycom virtual products for the VMware environment are distributed.

2. When using the Add Existing Instance feature, a Resource Group that does not exist when the instance is added is auto-generated and added to the zone to which the instance is assigned.
Since monitoring is a read-only action, the Read-Only role is sufficient to meet the need, and no additional permissions are necessary for RealPresence Resource Manager to obtain the information it requires to monitor VM instances.

**Recommendations**

The following categories of permissions provide specific functionality within RealPresence Resource Manager:

- A read-only role that covers the majority of the APIs used by RealPresence Resource Manager.
- A set of permissions for an instance management (power on, power off, and delete) role.
- A set of permissions for instance creation.

The union of the permissions listed above enables full functionality within the RealPresence Resource Manager system.

The next table provides guidance based on the restrictions in your organization for allowing a third-party application to control the virtualization solution. A more restricted vCenter environment causes some actions within the RealPresence Resource Manager system to fail with a permissions error.

Because RealPresence Resource Manager does not track permissions assigned to a specific vCenter role, it cannot allow or disallow actions within RealPresence Resource Manager. Restricted environments at the vCenter level can cause failures within RealPresence Resource Manager; however, such conditions are temporary and recoverable.

### Recommendations for vCenter Permissions in RealPresence Resource Manager

<table>
<thead>
<tr>
<th>Customer Environment</th>
<th>Role</th>
<th>Caveats</th>
</tr>
</thead>
<tbody>
<tr>
<td>No write access</td>
<td>Use predefined Read-Only in vCenter</td>
<td>Attempting to power on, power off, or delete an instance temporarily puts the instance into an Error state and makes license allocations unavailable for the instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Corrective Action: State will correct itself in 10 minutes or less. No other side effects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attempting to create an instance fails immediately.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Corrective Action: Delete the instance.</td>
</tr>
<tr>
<td>Limited write access (no ability to create, power up, power down, or delete)</td>
<td>Instance Management permissions only</td>
<td>Attempting to create an instance fails immediately.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Corrective Action: Delete the instance.</td>
</tr>
<tr>
<td>Full RealPresence Resource Manager functionality</td>
<td>Union of Instance Management and Instance Creation permissions</td>
<td>None. All permissions defined for all features in RealPresence Resource Manager.</td>
</tr>
</tbody>
</table>
Polycom, Inc. 567

Supported Ciphers

On the Admin > Management and Security > TLS Settings page, you can enable different ciphers suites and modes. RealPresence Resource Manager supports the following cipher options:

- Cipher Modes:
  - Strong Ciphers
  - Standard Ciphers
  - Weak Ciphers
- Enable Fips-140
- Enable CBC Ciphers
- Enable Static Ciphers

You can enable or disable the CBC and static ciphers in any cipher mode. For example, if you select Strong Ciphers with CBC Ciphers and Static Ciphers enabled, all the CBC, static, DHE, and ECDHE ciphers are enabled.

<table>
<thead>
<tr>
<th>Cipher Mode</th>
<th>NSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong Ciphers mode with CBC Ciphers and Static Ciphers enabled when RealPresence Resource Manager works as a server.</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256</td>
</tr>
</tbody>
</table>
**Cipher Mode** | **NSS**
--- | ---
**Strong Ciphers** mode with **CBC Ciphers** and **Static Ciphers** enabled when RealPresence Resource Manager works as a client.

- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
<table>
<thead>
<tr>
<th>Cipher Mode</th>
<th>NSS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supported Ciphers</strong></td>
<td><strong>SSL_rsa_with_3des_ede_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_ecdhe_rsa_with_3des_ede_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_ecdhe_rsa_with_aes_128_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_ecdhe_rsa_with_aes_256_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>SSL_dhe_rsa_with_3des_ede_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_rsa_with_aes_128_gcm_sha256,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_rsa_with_aes_256_gcm_sha384,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_dhe_rsa_with_aes_128_gcm_sha256,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_dhe_rsa_with_aes_256_gcm_sha384,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_dhe_rsa_with_aes_128_cbc_sha256,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_ecdhe_rsa_with_aes_128_cbc_sha256,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_ecdhe_rsa_with_aes_256_cbc_sha384,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_dhe_rsa_with_aes_256_cbc_sha256,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_rsa_with_aes_128_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_ecdhe_rsa_with_aes_128_gcm_sha256,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_ecdhe_rsa_with_aes_256_gcm_sha384,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_dhe_rsa_with_aes_128_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_rsa_with_aes_256_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_dhe_rsa_with_aes_256_cbc_sha,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_rsa_with_aes_128_cbc_sha256,</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TLS_rsa_with_aes_256_cbc_sha256</strong></td>
</tr>
<tr>
<td>Cipher Mode</td>
<td>NSS</td>
</tr>
<tr>
<td>-------------</td>
<td>-----</td>
</tr>
<tr>
<td><strong>Standard Ciphers</strong> mode with <strong>CBC Ciphers</strong> and <strong>Static Ciphers</strong> enabled when RealPresence Resource Manager works as a client.</td>
<td>TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_DSS_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA256</td>
</tr>
<tr>
<td>Cipher Mode</td>
<td>NSS</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Weak Ciphers</strong> mode with <strong>CBC Ciphers</strong> and <strong>Static Ciphers</strong> enabled when RealPresence Resource Manager works as a server.</td>
<td>SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td><strong>Weak Ciphers</strong> mode with <strong>CBC Ciphers</strong> and <strong>Static Ciphers</strong> enabled when RealPresence Resource Manager works as a client.</td>
<td>TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td><strong>FIPS-140</strong> mode when RealPresence Resource Manager works as a server.</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td><strong>FIPS-140</strong> mode when RealPresence Resource Manager works as a client.</td>
<td>SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
</tbody>
</table>