User Guide

Version 1.8 | Release Date (December 2014) | 3725-69907-005/A

Polycom® RealPresence® Capture Server, Appliance Edition
## Contents

**System Overview** .................................................................................................................. 7  
- Capacity ................................................................................................................................. 7  
- RealPresence Capture Server Stand-alone Unicast Live Streaming and VoD ..................... 9  
- RealPresence Capture Server and External Stream Servers ............................................... 10  
- Multi-user Login Capacity ....................................................................................................... 10  
- Local Media Storage Capacity .............................................................................................. 10  

**User Interfaces** ..................................................................................................................... 11  
- Web-based Admin Portal ......................................................................................................... 11  
- User Permissions through Admin Portal ................................................................................... 12  
- Web-based User Portal ............................................................................................................ 12  
- Search and Refresh Lists .......................................................................................................... 13  
- TV user interface (also called the "TVUI") .............................................................................. 13  
- Understand the Main Menu ..................................................................................................... 13  
- Console .................................................................................................................................. 14  

**Hardware Installation** ......................................................................................................... 15  
- Hardware Requirements ........................................................................................................ 15  

**Software Installation** ........................................................................................................... 17  
- Software Requirements .......................................................................................................... 17  
- Resource and License Management ....................................................................................... 17  
- Web Browser and OS Requirements ....................................................................................... 18  
- Set up RealPresence Capture Server in a Virtual Environment ............................................ 18  
- Configure NFS (Required) ...................................................................................................... 19  
- Product Activation .................................................................................................................. 20  
- Obtain the Product Activation Key from Polycom ................................................................. 20  
- Activate Product and Check the Activation Status ............................................................... 20  

**System Initialization** ............................................................................................................ 22  
- Configure IP Settings through Console ................................................................................... 22  
- Configure IP Settings through Admin Portal ......................................................................... 23  
- Configure the IP Parameters ................................................................................................. 23  

**System Administration** ....................................................................................................... 27  
- Check System Status on Home ............................................................................................... 27
Record and Playback ............................................... 49
  Configure Templates ........................................... 49
  Configure Recording Templates ................................. 49
  Configure Transcoding Template .............................. 53
  Configure VRRs .................................................. 55
  Start a Recording ............................................... 56
  Point-to-point Recording ...................................... 58
  Dial in from Endpoint ......................................... 58
    Record from RMX via Recording Link ....................... 59
    Change Conference Layout for MCU hosted calls ....... 59
    Dial into a VRR to Start Recording ....................... 59
  Play Back Media Archives .................................... 60
  Quick Code ..................................................... 61

Live Streaming/VoD .............................................. 63
  Streaming Using Capture Server ............................... 63
  Streaming Using External Servers ............................ 63
  Live Streaming .................................................. 67
    Start Live Streaming ......................................... 68
    Multi Live Streaming ......................................... 68
    View Live Streaming Information .......................... 68
    View Live Streaming Video ................................ 68

Media Management .............................................. 71
  Manage Archives ................................................ 71
  View Archive Details .......................................... 71
  Play Back and Download Archives ............................ 71
  Modify Archives ................................................ 73
  Dynamic Archiving ............................................. 73
  Transcoding .................................................... 74

Fault Management .............................................. 76
  System Log Configuration ..................................... 76
  Configure Log Settings ....................................... 76
  Log Management ............................................... 77
  Restart and Shut Down the System ............................ 77

Upgrade, Backup, Restore, and Migrate .......................... 80
  System Upgrade and Downgrade ................................ 80
  Backup and Restore ............................................ 81
Back Up and Restore Data .................................................. 81
Configure an FTP Server for Backup .................................. 82
Back Up and Restore Archives .......................................... 82

Manage Archives and Live Streams Using the User Portal .... 84
Manage Archives and Live Streams Using the User Portal ... 85
View Live Streams .............................................................. 86

Appendix A – Console Commands ........................... 87
Login Console ................................................................. 87
Console Command Descriptions .................................... 88
Help .............................................................. 88
Exit .............................................................. 88
Viewing Device Information ......................................... 88
Reboot Device ............................................................... 88
Power off System ............................................................ 88
Reset Password ............................................................. 89
Reset Admin Password ................................................ 89
Restore System Configuration ...................................... 89
Check Disk Space Usage ................................................. 89
Ping .............................................................. 90
Network Settings .......................................................... 90

Appendix B – Configure External Servers .............. 92
Live Stream Meetings to an External Media Server ........ 92
Configure the Wowza Media Server ............................... 93
Configure the IIS Media Server ....................................... 95
Configuring the Windows Media Server ...................... 99
View the Streaming through External Media Server .... 100

Appendix C – Configure the Server Working with VCS ... 102
Configure VCS Calling .................................................... 102
Configure VCS for SIP Calling ......................................... 102
This chapter introduces the important safeguards and regulatory notices.

**Important Safeguards**

Read and understand the following instructions before using the system:

- Close supervision is necessary when the system is used by or near children. Do not leave unattended while in use.
- Only use electrical extension cords with a current rating at least equal to that of the system.
- Always disconnect the system from power before cleaning and servicing and when not in use.
- Do not spray liquids directly onto the system when cleaning. Always apply the liquid first to a static free cloth.
- Do not immerse the system in any liquid or place any liquids on it.
- Do not disassemble this system. To reduce the risk of shock and to maintain the warranty on the system, a qualified technician must perform service or repair work.
- Connect this appliance to a grounded outlet.
- Only connect the system to surge protected power outlets.
- Keep ventilation openings free of any obstructions.
- If the system or any accessories are installed in an enclosed space such as a cabinet, ensure that the air temperature in the enclosure does not exceed 40°C (104° F). You may need to provide forced cooling to keep the equipment within its operating temperature range.
- Do not use this product near water.
- Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lighting.
- Only use this product below the altitude of 2000 meters.
- Only for the non-tropical climate conditions for safe use.
- No user serviceable parts are contained within the device.

The device contains a lithium cell. Risk of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacture. Dispose used batteries according to the manufacturer’s instructions.

This equipment is not to be installed in rack units that contain mounting slots at heights more than one meter.

SAVE THESE INSTRUCTIONS.
Regulatory Notices

USA and Canadian Regulatory Notices
This Class [A] digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe [A] est conforme à la norme NMB-003 du Canada.
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: This device may not cause harmful interference, and this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

In accordance with part 15 of the FCC rules, the user is cautioned that any changes or modifications not expressly approved by Polycom Inc. could void the user’s authority to operate the equipment.

EU Regulatory Notices
This RealPresence Capture Server system has been marked with the CE mark. This mark indicates compliance with EEC Directives 2006/95/EC and 2004/108/EC. A full copy of the Declaration of Conformity can be obtained from Polycom Ltd, 270 Bath Road, Slough, Berkshire, SL1 4DX, UK.

Russia Regulatory Information

<table>
<thead>
<tr>
<th>Система</th>
<th>Номер регистрации</th>
<th>Дата истечения срока</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Server</td>
<td>Д-СПД-6758</td>
<td>June 02, 2017</td>
</tr>
</tbody>
</table>

声明
此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

A 급 기기 (업무용 방송통신기자재)
이 기기는 업무용(A 급) 전자파적합기기로서 관계자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

WARNING
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.
Safety Considerations and Storage

- RealPresence Capture Server has a 7 year period of life.
- RealPresence Capture Server has a 7 year period of storage.

Electrical safety advisory
We recommend that you install an AC surge arrester in the AC outlet to which this device is connected. This action will help to avoid damage to the equipment caused by local lighting strikes and other electrical surges.

Special Safety Instructions
Follow existing safety instructions and observe all safeguards as directed.

<table>
<thead>
<tr>
<th>Environment</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating temperature</td>
<td>5° to 40°C (40° to 100°F).</td>
</tr>
<tr>
<td>Non-operating temperature</td>
<td>-40° to 5° (-40° to 40°F), 40°C to 60°C (100° to 140° F).</td>
</tr>
<tr>
<td>Operating Relative humidity</td>
<td>8% to 90% non-condensing.</td>
</tr>
<tr>
<td>Non-operating Relative humidity</td>
<td>5% to 8%, 90% to 95% non-condensing</td>
</tr>
</tbody>
</table>
System Overview

The Polycom® RealPresence Capture Server is a streaming and recording system that participates in standards-based video and telepresence calls that can be used alone or as an integrated component of Polycom Video Content Management solution. As a native part of the Polycom RealPresence Platform, the RealPresence Capture Server records, archives, and streams telepresence and video conferences for playback on a variety of client devices including tablets, smart phones, desktop computers, and standards-based video endpoints.

The RealPresence Capture Server is typically deployed as part of a larger Polycom RealPresence Platform solution, but it can be used as a standalone solution or with third-party systems. The Real Presence Capture Server’s full potential can best be realized when it is integrated with the Polycom RealPresence Media Manager.

By leveraging RealPresence Capture Server with existing telepresence systems, video conferencing endpoints and video infrastructure, or familiar unified communications (UC) tools, your organization can easily convert real-time conferences and events into reusable multimedia assets. Following are some features of RealPresence Capture Server:

- It integrates with Polycom endpoints, conference platforms, and other standards-based video endpoints for automated recording and playback.
- It supports H.323 and SIP standards for interoperability with third-party conferencing systems.
- It is available with several licenses that control the number of video calls that can be recorded, and of those calls, the number of calls that can be streamed live for viewing on web browsers.
- It can output a maximum stream (live or video on demand) of 1080p HD (people+content combined)
- It provides access to live and video call archive streams on devices with compatible browsers including PC, MAC, iOS, and Android devices.
- It enables you to access video call archives via any standard-based endpoint.
- It provides REST API support for third-party integrations.
Capacity

The license that you buy determines the RealPresence Capture Server capability. The following table shows the maximum capacity of the RealPresence Capture Server when it performs different features.

### RealPresence Capture Server Capacity

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Maximum Record Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>6/3 model</td>
</tr>
<tr>
<td>Signaling Connection (H323/SIP)</td>
<td>Specifies the maximum number of devices connected to RealPresence Capture Server simultaneously.</td>
<td>6</td>
</tr>
<tr>
<td>Conference Recording</td>
<td>Specifies the maximum number of devices that RealPresence Capture Server records simultaneously.</td>
<td>6</td>
</tr>
<tr>
<td>Playback (H323/SIP)</td>
<td>Specifies the maximum number of endpoints that can be connected to RealPresence Capture Server to view playback simultaneously.</td>
<td>6</td>
</tr>
<tr>
<td>Unicast Live Streaming and VoD</td>
<td>Specifies the maximum number of web connections support by RealPresence Capture Server to simultaneous view live streaming and/or VOD streaming.</td>
<td>Up to 500</td>
</tr>
</tbody>
</table>

### RealPresence Capture Server Capacity

<table>
<thead>
<tr>
<th>Capture Server Model</th>
<th># of Live Ports (720p)</th>
<th># of Recording/Playback Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Only</td>
<td>0</td>
<td>40</td>
</tr>
<tr>
<td>Minimum</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Medium</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>Maximum</td>
<td>9</td>
<td>18</td>
</tr>
</tbody>
</table>
Live Streaming Resources Usage

The combination of frame rate, resolution and number of live streaming rates used affects the quantity of resources required on the RealPresence Capture Server to support live streaming.

On Capture Server, streaming port calculation is used as quantitative indicator of live streaming resources, one stream (single bitrate) of 720p live streaming costs system resource calculated as one streaming port, for example, one stream of 1080p live streaming needs two streaming ports.

If multiple bitrates are configured for one live stream, each bitrate is calculated separately.

If WMV is configured as the output format and the layout is set as dual window, then one additional port is calculated as well for each bitrate.

In addition to live streaming, the following features also use streaming ports:

- Video call playback
  
  For details, refer to Video Call Playback.

- Point-to-point recording

Streaming ports are reserved before calls are connected by call rate in recording template.

If there are not enough streaming ports available in system for one service request, the request will be rejected. If real call rate is lower than the call rate configured in recording template, the Capture Server system will update the streaming ports that are really occupied. If system finds that multiple live streams are at the same rate, it will turn off duplicated live rates to save live streaming resources and occupied streaming resources.
ports will be updated together. If external live media server is configured in the VRR template, system will not turn off duplicate live rates.

**Resource Consumption**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Resources Consumed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording/Live Streaming resource consumed</td>
<td>Resolution</td>
</tr>
<tr>
<td>Conference Call (or Endpoint Call)</td>
<td>4CIF/SD</td>
</tr>
<tr>
<td></td>
<td>720p</td>
</tr>
<tr>
<td></td>
<td>1080p</td>
</tr>
<tr>
<td>Video Call Playback</td>
<td>4CIF/SD</td>
</tr>
<tr>
<td></td>
<td>720p</td>
</tr>
<tr>
<td></td>
<td>1080p</td>
</tr>
<tr>
<td>P2P</td>
<td>4CIF/SD</td>
</tr>
<tr>
<td></td>
<td>720p</td>
</tr>
<tr>
<td></td>
<td>1080p</td>
</tr>
</tbody>
</table>

**RealPresence Capture Server Stand-alone Unicast Live Streaming and VoD**

RealPresence Capture Server base system is licensed for 250 simultaneous viewing of live and VoD streams from the User Portal. RealPresence Capture Server system supports a maximum number of simultaneous live, or VoD streams, from the User Portal is 500, with the purchase of a stream upgrade option.

<table>
<thead>
<tr>
<th>Stream Rate on User Portal</th>
<th>Number of Simultaneous Streams from Capture Server User Portal</th>
<th>License</th>
<th>Upgradeable to Maximum Simultaneous Streams</th>
</tr>
</thead>
<tbody>
<tr>
<td>128 kbps–512 kbps</td>
<td>250 streams</td>
<td>Included with base system</td>
<td>500</td>
</tr>
<tr>
<td>768 kbps–1728 kbps</td>
<td>125 streams</td>
<td>Included with base system</td>
<td>250</td>
</tr>
<tr>
<td>2560 kbps</td>
<td>50 streams</td>
<td>Included with base system</td>
<td>100</td>
</tr>
</tbody>
</table>

**Multi-user Login Capacity**

The maximum number of Admin Portal session and User Portal session (including anonymous login) is as follows:
● Admin Portal Session: 200
● User Portal Session: 3000
Local Media Storage Capacity

Each 60 minutes 512k call to RealPresence Capture Server requires about 450M storage (the 512k call raw + the default mp4 VoD). For 1024k, the storage space is about double, which is 900M. You cannot calculate an accurate ratio because the size also depends on the video quality.

Storage Usage

<table>
<thead>
<tr>
<th>Situation</th>
<th>Primary Rate</th>
<th>Call Duration</th>
<th>Storage Space (WMV)</th>
<th>Storage Space (MP4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1*1080p</td>
<td>1024 kbps (MP4) 1728 kbps (WMV)</td>
<td>60 minutes</td>
<td>~1.4 GB</td>
<td>~870 MB</td>
</tr>
<tr>
<td>1*1080p</td>
<td>4096 kbps</td>
<td>60 minutes</td>
<td>~3.2 GB</td>
<td>~3.5 GB</td>
</tr>
<tr>
<td>1*720p</td>
<td>4096 kbps</td>
<td>60 minutes</td>
<td>~3.2 GB</td>
<td>~3.5 GB</td>
</tr>
<tr>
<td>1*720p</td>
<td>1024 kbps</td>
<td>60 minutes</td>
<td>~862 MB</td>
<td>~860 MB</td>
</tr>
<tr>
<td>1*4CIF</td>
<td>512 kbps</td>
<td>60 minutes</td>
<td>~458 MB</td>
<td>~459 MB</td>
</tr>
<tr>
<td>1*CIF</td>
<td>128 kbps</td>
<td>60 minutes</td>
<td>~100 MB</td>
<td>~103 MB</td>
</tr>
</tbody>
</table>

People Video | Content Video
--- | ---
Call Protocols | H.323, SIP | H.239, BFCP (TCP only)
Audio Protocols/Codes | G.711, G.722, G.722.1, G.722.1.C, G.729A, Siren 14 (Mono, Stereo), Siren 22 (Mono, Stereo), Siren LPR, Siren LPRStereo | N/A
## Approximate Capacity of Polycom Capture Server 1.7 in Hours of Recording

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Call speed (Kbps)</th>
<th>Approx. file size of 1 hour @MP4, in MB (from Admin Guide)</th>
<th>Approx. number of hours of recording/TB of storage</th>
<th>Approx. capacity of Capture Server Appliance Local storage, in hours (Capacity=3.5 TB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIF</td>
<td>128,000</td>
<td>103</td>
<td>9,700</td>
<td>33,950</td>
</tr>
<tr>
<td>4CIF/SD</td>
<td>512,000</td>
<td>459</td>
<td>2,170</td>
<td>7,595</td>
</tr>
<tr>
<td>720p30</td>
<td>1,024,000</td>
<td>860</td>
<td>1,160</td>
<td>4,060</td>
</tr>
<tr>
<td>1080p30</td>
<td>1,024,000</td>
<td>870</td>
<td>1,140</td>
<td>3,990</td>
</tr>
<tr>
<td>720p30</td>
<td>4,096,000</td>
<td>3,500</td>
<td>280</td>
<td>980</td>
</tr>
<tr>
<td>1080p30</td>
<td>4,096,000</td>
<td>3,500</td>
<td>280</td>
<td>980</td>
</tr>
</tbody>
</table>

* These values are all estimates because file size varies by call speed, video quality, and amount of motion. File size info from Admin Guide, capacity is per data sheet.
* Storage capacity can be expanded on appliances by using NAS storage.
* Capture Server Virtual Edition uses NAS storage exclusively.
User Interfaces

RealPresence Capture Server provides four interfaces that are used for specific purposes: Web-based Admin Portal, Web-based User Portal, TV User Interface, and Console.

Web-based Admin Portal

This section introduces how to access the web-based Admin Portal and its fundamental layout. You can access the Admin Portal via a compatible web browser and do the following:

- Configure the system.
- Set up recording parameters.
- Monitor system use and health.
- Dial out to endpoints to record meetings, disconnect calls in progress, and create different transcoded versions of archived calls.
- Download media files and give admin users a quick way to access and play archives and live streams.

RealPresence Capture Server system allows up to 200 users with admin rights to log in to the Admin Portal at the same time.

User Permissions through Admin Portal

You can log in to the Admin Portal as an administrator, an auditor or an user. The following table explains user permissions.

User Permissions

<table>
<thead>
<tr>
<th>Content</th>
<th>Auditor</th>
<th>Administrator</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessible information</td>
<td>System logs</td>
<td>All pages</td>
<td>Archives and live streaming.</td>
</tr>
<tr>
<td>Operation permissions</td>
<td>View and download system logs.</td>
<td>View, edit, and delete</td>
<td>Access archives, view live streaming and make recordings.</td>
</tr>
</tbody>
</table>

To log in to the Admin Portal:

1. In the address line, enter the system’s IP address in this format: https://<system IP address>/admin.
When an IPV6 address is used, refer to the following format:
https://[ipv6]/admin

2 Enter your user name and password to log in to the system.

To enhance security, Capture Server has changed the default from http to https. Request to RealPresence Capture Server system, sent to http://<system IP address>/admin> will be automatically redirected to https://system IP address/admin, for example, https://10.11.12.13/admin. Using the HTTPS protocol ensures that the configuration of all login credentials (such as user names and passwords) are transmitted using an encrypted channel. This includes those credentials used to communicate with third-party systems on your network. Using the HTTPS protocol limits the ability of anyone monitoring traffic on the network to discover these credentials.

Web-based User Portal
Accessed via compatible device/web browser (PC/MAC, iOS and Android), the User Portal offers the following functions:

- Find, navigate, and search items.
- Play archives and live streams.
- Make calls.

Search and Refresh Lists
You can search items listed on the User Portal, for example, archives and live streaming.

To search for a target item in the list:

» Enter the name, or part of the name of the entry you want to find in the text field, and then click .

- Keyword search is not case sensitive.
- In the archives search box, you can also type the keywords specified to an archive.
- If you want to return to the full list view, delete all characters in the text field and click .

To refresh the list:
Click the icon displayed above the list.

TV user interface (also called the “TVUI”)
Accessed via standards-based video conferencing endpoints, this interface can be used to record meetings, control recording and playback.
Understand the Main Menu

In addition to the Admin Portal, the RealPresence Capture Server system also provides a TV user interface for you to perform the most commonly used operations. The TV user interface appears after an endpoint dials the RealPresence Capture Server system and sets up a connection successfully.

**TV User Interface**

After the endpoint sets up connection with the RealPresence Capture Server system, it enters the TV user interface menu page, where common recording and playback options are provided, as shown below.

If the **Start Recording Immediately** function has been enabled in the VRR used by the endpoint for dialing, the endpoint enters **Recording Status** directly. You can control the RealPresence Capture Server system using the FECC and DTMF functions of the remote control. When your endpoint supports FECC or DTMF, use the remote control to operate the TV user interface menu page.

The table below defines in detail the FECC and DTMF operation keys on the remote control of Polycom endpoint.

**FECC and DTMF Operation Keys**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>FECC</th>
<th>Description</th>
<th>DTMF</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When in the menu display state</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>⏸</td>
<td>Pause the recording</td>
<td>*1</td>
<td>Pauses the recording</td>
</tr>
<tr>
<td></td>
<td>⏪</td>
<td>Confirm the selection</td>
<td>*2</td>
<td>Starts or resumes a paused recording</td>
</tr>
<tr>
<td></td>
<td>⏪</td>
<td>Select leftward (cyclic).</td>
<td>*3</td>
<td>Stops the recording.</td>
</tr>
<tr>
<td></td>
<td>⏬</td>
<td>Select rightward (cyclic).</td>
<td>*5</td>
<td>Plays back the recording.</td>
</tr>
</tbody>
</table>
### Console

Accessed via VGA interface or SSH, console is used to view/change IP settings and reboot the system. For example, set DNS server, view disk space usage and shut down the system.

Refer to Appendix A for more supported command line information.

<table>
<thead>
<tr>
<th>When in the video playing state</th>
<th>-</th>
<th>-</th>
<th>*1</th>
<th>Pauses the current video.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-</td>
<td>-</td>
<td>*2</td>
<td>Starts or resumes a paused video.</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>-</td>
<td>*3</td>
<td>Stops playback of the current video and returns to the main menu.</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>-</td>
<td>*4</td>
<td>Reverses the current video.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>*6</td>
<td>Fast forwards the current video.</td>
</tr>
</tbody>
</table>
Hardware Installation

Capture Server Front Panel  The front panel of the Polycom RealPresence Capture Server system is shown in the next illustration.

There are two buttons located on the front of the chassis as below:

<table>
<thead>
<tr>
<th>Button</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reset</td>
<td>Use the reset button to reboot the system.</td>
</tr>
<tr>
<td></td>
<td>Power ON/OFF</td>
<td>This is the main power button, which is used to apply or turn off the main system power. Turning off system power with this button removes the main power but keeps standby power supplied to the system.</td>
</tr>
</tbody>
</table>

There are six LEDs located on the front of the chassis as below:

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
<th>Panel Identifier</th>
<th>Status</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN1</td>
<td>LAN1 Activity Status Indicator</td>
<td>🌍</td>
<td>Link</td>
<td>Green</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Activity</td>
<td>Green Blink</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No Link</td>
<td>Off</td>
</tr>
</tbody>
</table>
There are four HDDs located on the front of the chassis as below:

<table>
<thead>
<tr>
<th>No.</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HDD 1</td>
<td>Hard Disk 1 for storage data</td>
</tr>
<tr>
<td>2</td>
<td>HDD 2</td>
<td>Hard Disk 2 for storage data</td>
</tr>
<tr>
<td>3</td>
<td>HDD 3</td>
<td>Hard Disk 3 for storage data</td>
</tr>
<tr>
<td>4</td>
<td>HDD 4</td>
<td>Hard Disk 4 for storage data</td>
</tr>
</tbody>
</table>

**Capture Server Rear Panel**

The Capture Server rear panel contains built-in power and fan units, USB, LAN, VGA and serial port.
Capture Server rear panel

<table>
<thead>
<tr>
<th>No.</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power socket and fan</td>
<td>Built-in power socket and fan</td>
</tr>
<tr>
<td>2 (optional)</td>
<td>Power socket and fan</td>
<td>Built-in power socket and fan</td>
</tr>
<tr>
<td>3</td>
<td>Serial (RS 232)</td>
<td>Disabled</td>
</tr>
<tr>
<td>4</td>
<td>USB 1</td>
<td>For USB device connection</td>
</tr>
<tr>
<td>5</td>
<td>USB 2</td>
<td>For USB device connection</td>
</tr>
<tr>
<td>6</td>
<td>USB 3</td>
<td>For USB device connection</td>
</tr>
<tr>
<td>7</td>
<td>USB 4</td>
<td>For USB device connection</td>
</tr>
<tr>
<td>8</td>
<td>LAN 1</td>
<td>For management network connection when network separation is enabled. By default, LAN1 is for all management, signaling and media network connections.</td>
</tr>
<tr>
<td>9</td>
<td>LAN 2</td>
<td>For signaling network connection when network separation is enabled. LAN2 is disabled by default.</td>
</tr>
<tr>
<td>10</td>
<td>VGA</td>
<td>Diagnostics only</td>
</tr>
</tbody>
</table>

### Hardware Specifications

The following table shows the hardware specifications for the RealPresence Capture Server.

#### Hardware Specifications

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Dual Intel® E5-2620 (single for China 6/3 port license) @ 2.0 GHz 12 cores Note: The hyper-thread core is 24.</td>
</tr>
<tr>
<td>RAM</td>
<td>32GB (16 GB for China 6/3 port license) DDR3 ECC Registered memory</td>
</tr>
</tbody>
</table>
Hardware Installation

Before you begin installing this product, make sure you follow these rules to ensure general safety:

- Keep the area around the RealPresence Capture Server unit clean, free of clutter, and well ventilated.
- Choose a suitable location for the equipment rack that will hold the unit and ensure that it is near a grounded power outlet.
- Use a regulating UPS (uninterruptible power supply) to protect the RealPresence Capture Server unit from power surges and voltage spikes, and to keep it operating in case of a power failure.

Unpack the Package

When you unpack the RealPresence Capture Server package, ensure check to be sure that the following items are included:

- One RealPresence Capture Server appliance (weighs about 50 lbs)
- Rail-mount kit for standard 19-inch equipment rack
- One power cable for your regional power
- Two RJ-45 network cables
- Documentation DVD, which contains the links to the latest RealPresence Capture Server documentation on the Polycom Support web site
- A piece of paper containing the license information.

Inspect all items in the package to ensure they are in proper working condition.

If you find damage, file a claim with the delivery carrier. Polycom is not responsible for damage sustained during shipment of this product.

Install RealPresence Capture Server

After you unpack and examine the product package and remove all of the components from their containers, you can install the product.

To install RealPresence Capture Server:

1. Place the RealPresence Capture Server unit on a stable flat surface.
2  Peel off the protective film from the top and bottom of the appliance.
3  If appropriate, install the rack-mount rail kit following the instructions provided.
4  Place the appliance in a properly ventilated equipment rack (shelf or rails) or similar environment.
5  Insert the power cable connector into the rear of the chassis and connect it to an appropriately rated socket outlet.
6  Connect a network cable to LAN 1 on the back of the unit.
7  Power on the system.

To isolate the equipment during servicing or any time you need to physically move the appliance, if a second power supply is installed with the redundancy kit, then both power cords must be disconnected. Otherwise, the system remains energized, even with only one plug connected.
Software Installation

Web Browser and OS Requirements

The following table lists the requirements on your computer to access the Admin Portal and User Portal.

User Portal Web Browser Requirement

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browser Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC (Windows 7, and Windows 8)</td>
<td>Internet Explorer</td>
<td>9, 10, 11</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>32, 33</td>
</tr>
<tr>
<td></td>
<td>Chrome</td>
<td>38, 39</td>
</tr>
<tr>
<td>MAC OS-X (Intel-based Leopard, Snow, and Lion)</td>
<td>Safari</td>
<td>7.1, 8.0</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>32, 33</td>
</tr>
<tr>
<td></td>
<td>Chrome</td>
<td>38, 39</td>
</tr>
<tr>
<td>iOS 7, 8</td>
<td>Safari</td>
<td>7.1.2, 8.1.1</td>
</tr>
<tr>
<td>Andriod phone and tablet</td>
<td>Android browser</td>
<td>4.3, 4.4.2</td>
</tr>
</tbody>
</table>

Product Activation

You must have a license to use the RealPresence Capture Server. The license type determines RealPresence Capture Server capability.

- RealPresence Capture Server - 6/3
  RealPresence Capture Server records up to 6 SIP or H.323 calls (up to 3x720p live streaming). It supports both MP4 and WMV formats.
● RealPresence Capture Server - 12/6
  RealPresence Capture Server records up to 12 SIP or H.323 calls (up to 6x720p live streaming). It supports both MP4 and WMV formats.

● RealPresence Capture Server - 18/9
  RealPresence Capture Server records up to 18 SIP or H.323 calls (up to 9x720p live streaming). It supports both MP4 and WMV formats.

● RealPresence Capture Server - 40/0
  RealPresence Capture Server records up to 40 SIP or H.323 calls, none of the calls can be used as live streams.

● Capacity license can be added to the 6/3 or 12/6 models to a maximum capacity of 18/9.

**Obtain the Product Activation Key from Polycom**

You must activate the license shipped with your order with the product serial number (you can find this by choosing **Admin > Product Activation**) identified within RealPresence Capture Server.

**To obtain the product activation key:**

1. Obtain the serial number from rear panel of the Capture Server system. Write it down for later use.
2. Enter the following web site address in the address bar of the web browser: support.polycom.com. and go to **Support Home**.
3. Go to **Licensing & Product Registration > Activation/Upgrade**.
4. Click **All other Polycom Products** in the pop-up window.
5. Enter your e-mail address and password to log in to or register for a new account.
6. Follow the page prompts step by step to generate the Key Code required for system activation.
7. Enter the **Serial Number** you recorded and click **Next**.
8. Follow the page prompts step by step to generate the Key Code required for system activation. Enter the product options license numbers.
9. Note down the activation key (Key Code) on the page and click **Upgrade**.
10. Go back to Capture Server Admin Portal and activate the system under **Admin > Product Activation**.

**To view the system activation status:**

» Go to **Admin > Product Activation**. The following system information is displayed:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Type</td>
<td>Permanent license</td>
</tr>
<tr>
<td>Software Version</td>
<td>Current version of the software running on the system</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Product serial number</td>
</tr>
<tr>
<td>Activation Status</td>
<td>Whether the system is activated; [☑] indicates activated system, and [☒] indicates it is not activated</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max Recording Ports</td>
<td>Maximum number of recording ports supported by the system</td>
</tr>
<tr>
<td>Max Live Streaming Ports</td>
<td>Maximum number of live streaming ports supported by the system</td>
</tr>
<tr>
<td>Max Streaming Sessions</td>
<td>Maximum number of video-on-demand and live streaming sessions supported by the system. Base: 250. Note: After purchasing and activating the license, the streaming sessions capacity will be increased from 250 to 500.</td>
</tr>
<tr>
<td>Media Encryption</td>
<td>Whether the AES encryption function of the system is activated. This is a charged function. You can use it only after purchasing the license and activating it.</td>
</tr>
<tr>
<td>Streaming without recording (no archive)</td>
<td>Whether the streaming without recording function of the system is activated. Once this function is activated, the system performs live streaming without recording and no archives left.</td>
</tr>
<tr>
<td>Timecode Watermark</td>
<td>Whether the basic timecode watermark capability for transcoded mp4 on-demand files is activated. On-demand archives can be output with basic timecode watermarking.</td>
</tr>
</tbody>
</table>
System Initialization

Fast Configuration Wizard

The Fast Configuration Wizard pops up if **Product Activation** is not done, it gets you up and running as soon as possible, all settings in the wizard can be changed later on under the various configuration pages.

**Step 1: Product Activation**

The basic system information is displayed here
For configuration steps, refer to **Product Activation**
Note: The Product Activations page must be filled out before you can continue, make sure the license is available when installing.

**Step 2: Configure IP Settings**

The RealPresence Capture Server system supports both IPv4 or IPv4 & IPv6 network communications. You can configure parameters to be used for network communication, including system IP address, DNS server, and NAT server.

For configuration steps, refer to **To set IP:**
If you are done with configuration, click **OK** to save the changes.

**Step 3: Configure Media Storage Settings**

By default, RealPresence Capture Server stores your archives on its local hard disk and network file system
For configuration steps, refer to **Configure Media Storage Settings**

**Step 4: Configure Signaling Settings**

For H.323, if a gatekeeper is configured on your network, you can register RealPresence Capture Server to the gatekeeper to simplify calling. A gatekeeper manages functions such as bandwidth control and admission control. A gatekeeper also handles address translation, which allows you to make calls using static aliases instead of IP addresses that may change each day.
If you make SIP calls, you can register RealPresence Capture Server to a SIP server to simplify calling.

For configuration steps, refer to **Configure Signaling Settings**
Step 5: Configure System Time

You also can set the RealPresence Capture Server system time from the Fast Configuration Wizard

For configuration steps, refer to Set the System Time

Configure IP Settings through Console

You can configure IP settings from either Capture Server system’s Console or Admin Portal.

To set the system IP address in the RealPresence Capture Server’s console:

1. Connect a VGA monitor to VGA interface of the RealPresence Capture Server system, and connect the USB keyboard to the USB interface of the Capture Server system.
2. Open the console of your RealPresence Capture Server.
3. The default console display is shown in the next illustration

![Console Display](image)

4. The IP address displayed on console is shown in the above illustration, the default IP address is https://192.168.1.254
5. Assign the system a static IP from the RealPresence Capture Server’s console.
6. Type Alt+F2 keys to go to the login screen.
7. Enter the user name and password (both are polycom by default).
8. Set RealPresence Capture Server a static IP or DHCP for LAN interface using Network Settings command, refer to Network Settings for details.
   Note: After you are finished with DHCP setting configuration, go to console and get the IP address information assigned by DHCP server.
9. After you set the IP, the Capture Server system will ask if you want the changes, click Yes to reboot.
Configure IP Settings through Admin Portal

The RealPresence Capture Server system supports both IPv4 or IPv4 & IPv6 network communications. You can configure parameters to be used for network communication, including system IP address, DNS server, and NAT server.

The RealPresence Capture Server system supports IPv6 system management.

To set IP:

1. Go to Configuration > IP Settings and configure the following settings:

Set IP Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Network Separation</td>
<td>Select this check box to route the management, streaming traffic and video call traffic through LAN 1 and LAN 2 interfaces separately. This offers higher security for the signaling data.</td>
</tr>
<tr>
<td>Obtain an IP Address Automatically (DHCP)</td>
<td>If you select this radio button, RealPresence Capture Server obtains an IPv4 address automatically via DHCP. <strong>Note:</strong> Obtaining an IP address automatically is not recommended. For best results, assign a static IP to RealPresence Capture Server.</td>
</tr>
</tbody>
</table>
| Using the following IP Address | • **IP Address**: the IP address of the system.  
• **Subnet Mask**: the subnet mask of the system.  
• **Default IPv4 Gateway**: the address of the interface to use for accessing the IPv4 gateway.  
• **Preferred DNS Server**: the preferred DNS server address for the system to resolve domain names.  
• **Alternate DNS Server**: the alternate DNS server address for the system to resolve domain names. |
| Enable IPv6 | Specify whether to enable IPv6 related functions. |
| Obtain an IP Address Automatically (IPv6) | Specify whether to obtain the IPv6 address automatically using Stateless Address Auto-configuration (SLAAC). **Note:** Obtaining an IP address automatically is not recommended. For best results, the system should be configured with a static IP address. |
| Using the following IP Address (IPv6) | Select this option to manually configure a static IPv6 address:  
• **Link Local Address**: Specify an address for link local communication. Routers do not forward packets with link local addresses.  
• **Site Local Address**: Specify an address for site local communication. Routers do not forward packets with site local addresses.  
• **Global Address**: Specify one or several address for communication with external IPv6 networks. Separate several addresses with a comma (,).  
• **Default IPv6 Gateway**: Specify the address of the interface to use for accessing the IPv6 gateway. |
2 Configure the following general settings:

**General System Network Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Specify the host name of the system.</td>
</tr>
<tr>
<td>Domain</td>
<td>Specify the domain name of the system.</td>
</tr>
</tbody>
</table>

3 Click **Add** to add static routes. You need to enter the following information for each route:

**Set Route Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Specify the IP address of the destination network.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Specify the IP address of the gateway to access the destination network.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify the subnet mask for the destination network.</td>
</tr>
</tbody>
</table>

4 Click **OK**. The system restarts to apply your changes.
System Configuration

This section explains the functions used for system administration in detail.

Check System Status on Home

You can find real time system status and information on Home.

Signaling Connection

Shows connection information and recording status of the calls to and from video endpoint or MCUs with this Capture Server. Click to expand detailed parameters information. The table below provides parameters descriptions.

Signal Connection Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Far End Number</td>
<td>The far end number used by the connection.</td>
</tr>
<tr>
<td>Start Time</td>
<td>When the calls started.</td>
</tr>
<tr>
<td>Signaling Type</td>
<td>H.323 or SIP.</td>
</tr>
<tr>
<td>Dial In/Out</td>
<td>Whether the connection is incoming or outgoing.</td>
</tr>
<tr>
<td>VRR Number</td>
<td>The VRR number used by the connection.</td>
</tr>
<tr>
<td>Live Streaming</td>
<td>Whether the connection is performing live streaming.</td>
</tr>
<tr>
<td>Detail</td>
<td>Additional information like VRR name, audio type, audio call rate, video type, video call rate, etc.</td>
</tr>
<tr>
<td>Real Time Information</td>
<td>Displays call address, audio packet loss, video resolution, video frame rate, etc.</td>
</tr>
</tbody>
</table>

You can control the recording using the controls:

- ● : Start recording.
- ● : Pause recording.
- ● : Resume recording.
- ● : Stop recording.
- ● : End the connection.

You can dial out to connect the endpoint to record using Dial out to record.
You can control the Quick Code playback using the controls:

- ● : Pause playback.
- ● ➤ : Resume playback.
- ● ■ : Stop playback.
- ● ➡ : Start playback.
- ● ◀ : Fast backward playback.
- ● ▶ : Fast forward playback
- ● 📡 : End the connection.

You can control the RMX playback using the controls:

- ● : Pause playback.
- ● ➤ : Resume playback.
- ● ■ : Stop playback.
- ● ◀ : Fast backward playback.
- ● ▶ : Fast forward playback
- ● ☰ : Change conference layout
- ● 📡 : End the connection.

**System Information**

Displays following system basic information:

- System name
- The current version of the software running on the system.
- The maximum number of recording ports and live streaming ports supported by the system.
- Recording ports and live streaming ports usage.

**System Alerts**

Shows the system alert information, for example, registration to primary gate-keeper failed, LAN2 failed to acquire DNS automatically, IP address conflict for LAN1, CPU usage is too high, memory usage is too high, NFS connection is lost, temperature is out of range, log size has reached the threshold value, etc.

**Signaling Server Status**

Displays gatekeeper registration status and SIP server registration status. When the H.323 registration is successful, the system’s E.164 prefix and H.323 alias are displayed.

**Hardware Status**

The following table shows the indicators and the hardware status in general. You can check the following status:

- Basic
System Configuration

- CPU Usage
- Memory Usage
- System Disk Usage
- Extension: Specifies value, total storage and status for RAID, disk, local media disk, power, etc.

Web Connections
Displays connection status on both Admin and User Portal for administrators, users, auditors, and anonymous users.

- Admin Portal Connections:
  - Current Administrators
  - Current Users
  - Current Auditors
- User Portal Connections:
  - Current Administrators
  - Current Users
  - Current Anonymous

External Server Status
The system can be integrated with external servers, such as IIS and WOWZA. You can check the configuration for IIS, WOWZA, Windows Media Server, AKAMAI, AD server and NFS server respectively.

Note: Make sure the NFS server is set up beforehand.

Manage Users and Groups
This section explains how to manage users.

User Roles
Users who are defined in the RealPresence Capture Server system can log in to the system’s Admin Portal to complete authorized operations. The system supports three user roles:

- Auditor: Who can only audit and manage system logs and set personal information.
- Administrator: Who can perform the most operations, and can view and configure all pages.
- User: Who can access archives and view live streaming.

Add a New User
You can add a local user to the system.

To add a local user:
1. Go to User > Users.
2. Click Add.
### System Configuration

3. Configure the following settings (* indicates mandatory options):

#### Adding an User

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Specify the user ID used for web login. User ID must be unique with a length of 1-128 characters, and consist of alphanumeric or &quot;_&quot; symbol characters. Once created, user ID cannot be modified.</td>
</tr>
<tr>
<td>Full Name</td>
<td>Specify the user's full name.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the login password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Specify the confirmed password which must be identical to the login password.</td>
</tr>
<tr>
<td>Role</td>
<td>User roles: Administrator, Auditor or User. Different roles determine the user operation permissions after logging in to pages.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify additional related information.</td>
</tr>
</tbody>
</table>

#### Modify User Information

The administrator can modify local user information and password, or delete user.

**To modify user information:**

1. Go to **User > Users**.
2. Select the user entry you want to edit.
3. Click **Edit**.
4. Enter the user information, and then click **OK**.

**To modify user password (local user only):**

1. Go to **User > Users**.
2. Select the user entry you want to modify.
3. Click **Change Password**.
4. Enter the new password and confirm password, then click **OK**.

After the password is changed by the administrator, the user is required to change the password when he logs in to the system using that password for the first time.

**To delete a user:**

1. Go to **User > Users**.
2. Select the user entry you want to delete.
3. Click **Delete**.
Create and Manage Groups

You can create user groups and set permissions for groups.

A default group, named all-users, is built in the system. It includes all the users defined in the RealPresence Capture Server system. All-users group cannot be modified or deleted. Administrators can define a new group, modify or delete existing groups.

To view user groups:
1. Go to User > Groups.
2. Filter by Local Groups or AD Groups.

To create a new user group:
1. Go to User > Groups.
2. Click Add.
3. Specify a name for the group. The group name must be unique. You can enter associated descriptions if necessary.
4. Click Group Members.
5. Select users to add to the group, and then click Add.
   To delete an item, select it and click Delete.

To modify or delete an existing group:
1. Go to User > Groups.
2. Select the group entry you want to delete.
3. Click Edit or Delete.

Set Recording Parameters

You can configure supplementary recording settings from Configuration > Call Settings. The system call setting will be applied as default value to all calls in the system. If there is difference in recording template, then usually recording template setting will take precedence.

To configure recording setting options:
1. Go to Configuration > Call Settings.
2. Configure the following settings:

### Record Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow recording even when no resources are available to create live stream(s).</td>
<td>If this option is selected, when there are insufficient resources available to live stream a meeting, the system records the meeting to the hard disk automatically. You cannot continue viewing the video in real time through the web. However, you can play back the video upon the completion of recording and format conversion. If this option is not selected, when there are no live streaming resources, the system rejects all calls that have live streaming enabled.</td>
</tr>
<tr>
<td>Key Frame interval</td>
<td>Specify the fast forward and backward intervals when playing back recorded files on an endpoint. For example, if it is set to one minute, the system inserts an index marker every minute when recording. When you press <strong>Fast forward</strong> using FECC (Far End Camera Control) or DTMF, the video playback jumps to the nearest index marker from the current location. Shorter intervals result in larger archive.</td>
</tr>
<tr>
<td>Indication Tone</td>
<td>Played to indicate that recording is ongoing, typically it is a very short beep with intervals between beeps, measured in second.</td>
</tr>
</tbody>
</table>
| Media Encryption | If the Capture Server is licensed for call encryption, this option specifies how AES (Advanced Encryption Standard) encryption is enabled and SIP connections:  
  - **Required For All Calls**: Enable the AES encryption for all H.323 and SIP calls, including video and audio only calls. This option requires the device to connect the system with AES enabled, otherwise, the connection cannot be set up.  
  - **When Available**: Enable the AES encryption and SIP connections when the peer device enables the AES option, and vice versa.  
  - **Off**: Disable the AES encryption and SIP connections. |
| Support AES 256-Bits key for encryption | If the Capture Server is licensed for call encryption, this option specifies whether to enable the 256-bit key for AES encryption. If not selected, the AES uses 128-bit key for encryption by default. |
| Max Call Length | The maximum call length for recording calls. The value is 4 hours by default. Note: Valid call length ranges from 1 to 8 hours. |
| Max Call Length (for streaming only call) | The maximum call length for streaming only calls. The value is 8 hours by default. Note: There is no limitation to this option. |
| Enable all IVR notifications | Enable IVR service at system level, the default left time to play IVR is 10 minutes. |
| Enable Global Quickcode Playback PIN | Enable quickcode playback PIN at system level. Note: If a PIN code is set under archive properties, the individual PIN code will override that set at system level. |
Configure Signaling Settings

For H.323, if a gatekeeper is configured on your network, you can register RealPresence Capture Server to the gatekeeper to simplify calling. A gatekeeper manages functions such as bandwidth control and admission control. A gatekeeper also handles address translation, which allows you to make calls using static aliases instead of IP addresses that may change each day.

If you make SIP calls, you can register RealPresence Capture Server to a SIP server to simplify calling.

H.323

If your network supports H.323, you can register RealPresence Capture Server to a H.323 server to simplify calling.

To register the system to a gatekeeper to make H.323 calls:

1. In the address line, enter the system’s IP address in this format: https://<system IP address>/admin.
2. Go to Configuration > Signaling Settings > H.323.
3. Select Register To Gatekeeper.
4. Configure the settings listed in the following table. After you finish the configuration, click OK.

H.323 Gatekeeper Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatekeeper type</td>
<td>Choose between Polycom and Cisco VCS.</td>
</tr>
<tr>
<td>Primary Gatekeeper</td>
<td>Indicates whether the system is registered to the primary gatekeeper.</td>
</tr>
<tr>
<td>Gatekeeper Address</td>
<td>Specify the IP address for the gatekeeper. Note: Never enter Capture Server's IP address.</td>
</tr>
<tr>
<td>Gatekeeper Port</td>
<td>Specify the port number for the gatekeeper, the default value is 1719.</td>
</tr>
<tr>
<td>Register User Information for Gatekeeper</td>
<td>Specify whether to register the system to a Polycom Gatekeeper server for H.235.0 authentication. When H.235.0 authentication is enabled, the gatekeeper ensures that only trusted endpoints are allowed to access the gatekeeper.</td>
</tr>
<tr>
<td>Gatekeeper User</td>
<td>Specify the user name for registration with the Polycom Gatekeeper server.</td>
</tr>
<tr>
<td>Gatekeeper Password</td>
<td>Specify the password for registration with the Polycom Gatekeeper server.</td>
</tr>
<tr>
<td>Alternate Gatekeeper</td>
<td>Indicates whether the system is registered to the alternate gatekeeper.</td>
</tr>
<tr>
<td>System Prefix / E.164</td>
<td>Specify the E.164 number for the system.</td>
</tr>
</tbody>
</table>

Note: The alternate gatekeeper is used only when the primary gatekeeper is not available.
System Configuration

Polycom, Inc.

SIP

If your network supports SIP, you can use SIP to connect video calls. RealPresence Capture Server supports SIP integration with SIP servers such as the Polycom DMA.

To configure the SIP settings:

1. Go to Configuration > Signaling Settings > SIP.
2. Configure the following settings:

**SIP Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System H.323 Alias</td>
<td>Specify the H.323 alias for the system.</td>
</tr>
<tr>
<td>Remote Display Name</td>
<td>Specify the name to be displayed to the far end.</td>
</tr>
<tr>
<td></td>
<td>Note: If you set the remote display name with dual-bytes characters like</td>
</tr>
<tr>
<td></td>
<td>Chinese, you will not see the characters on the far end endpoints in a</td>
</tr>
<tr>
<td></td>
<td>H.323 call between endpoints and the Capture Server system.</td>
</tr>
</tbody>
</table>

If the RealPresence Capture Server is registered to DMA as gatekeeper, you can find Capture Server's information on DMA portal under **Network > MCU > MCUs**.

**Parameter**

- **Transport Type**
  - Specify the transport layer protocol used for communicating with the SIP server. It needs to be consistent with the protocol supported by the SIP server.

- **Enable Certificate Validation**
  - Specify whether to validate the server's certificate before accepting it. This option is available only after you select TLS as the **Transport Type**.
  - **Note**: RealPresence Capture Server always sends its own certificate to the server, regardless of the selection here.

- **Register to SIP Server**
  - Specify whether to register the system to the SIP server.

- **SIP Server Type**
  - Choose a SIP server type from the dropdown list, currently only **Generic** available.

- **SIP Server status**
  - Specify:
    - **Server Address**
    - **Server Port**
    - **Server Domain Name**
  - **Note**: Never enter Capture Server IP for **Server Address**.

- **Register User's Information**
  - Specify:
    - **User Name**
    - **Auth User Name**
    - **User Auth Password**
Configure Port Settings

Port Settings allow specific ports in the firewall network environment to be allocated to multimedia calls.

To configure the port:

1. Go to Configuration > Port Settings.
2. Select Enable port configuration.
3. Configure the following settings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Ports</td>
<td>Specify the TCP port range. You can set the starting port number (the default value is 10000), and the ending port number is calculated automatically.</td>
</tr>
<tr>
<td>UDP Ports</td>
<td>Specify the UDP port range. You can set the starting port number (the default value is 20000), and the ending port number is calculated automatically.</td>
</tr>
<tr>
<td>Streaming Port</td>
<td>Specify the streaming port range. The default value is 1640.</td>
</tr>
<tr>
<td>Multicast Port</td>
<td>Specify the multicast port range. The default value is 1641.</td>
</tr>
</tbody>
</table>

4. Click OK. The recording server restarts to apply your changes.

Set the System Time

You also can set the RealPresence Capture Server system time from the Admin Portal.

To set the system time:

1. Go to Configuration > System Time.
2 Configure the following settings:

**System Time Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Service</td>
<td>Specify how to set the system time:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Console</strong>: Synchronize the system time with your computer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NTP Server</strong>: Obtain the system time from a time server.</td>
</tr>
<tr>
<td>Date</td>
<td>The current system date and time.</td>
</tr>
<tr>
<td>Time</td>
<td>Changing the time manually is not recommended.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The current time zone.</td>
</tr>
<tr>
<td>The NTP servers 1 and</td>
<td>Specify the address or domain name of a network time server. NTP server 2</td>
</tr>
<tr>
<td>The NTP server 2</td>
<td>is used only when NTP server 1 is not available.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you set a domain name, make sure you have already set a DNS</td>
</tr>
<tr>
<td></td>
<td>server address that can resolve this domain name in <strong>Configuration &gt; IP</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Settings</strong>.</td>
</tr>
</tbody>
</table>

3 Click **OK**. The system restarts to apply your changes.

**Configure Media Storage Settings**

By default, RealPresence Capture Server stores your archives on its local hard disk and network file system could be configured.

To save your files on a network file system:

1 Click **Configuration > Media Storage Settings**.
2 Choose from the listed Media Storage policies.
   - If select policy other than **“Local Storage First”**, you need to configure following settings for network file system.
3 Configure the following settings for the network file system.

**Media Storage Setting**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Server Name</td>
<td>Enter a name for the NFS server.</td>
</tr>
<tr>
<td>NFS Server Address</td>
<td>Enter an address of the NFS server.</td>
</tr>
<tr>
<td>NFS Storage Folder</td>
<td>Specify the folder path to the NFS storage.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Make sure the NFS server is set up beforehand.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the NFS server is reachable.</td>
</tr>
</tbody>
</table>
Configure Multicast Settings

The Polycom RealPresence Capture Server system supports the multicast function and can perform the one-to-many transmission of video streams. The system only needs to send the video streams once so that multiple computers can simultaneously share live streaming so as to greatly reduce the demand for transmitting network video streams and save the network bandwidth.

The Polycom RealPresence Capture Server system supports the simultaneous multicast of up to 100 channels.

**Before You Start**

To use the multicast function successfully, the following conditions are required to be met:

- The multicast function is activated in the Polycom Capture Server system. Contact your supplier to obtain this function.
- Routers and switches in the network of client computers are configured correctly to support the IP multicast communication with the Polycom Capture Server system.

**Configure Multicast**

Before you use the system to perform the multicast, it is necessary to configure parameters on the Multicast page.

**To configure multicast parameters:**

1. Go to **Configuration > Multicast Settings**.
2. Configure the following settings:
Multicast

The Polycom RealPresence Capture Server system supports the video multicast function and can send video streams to a group of computers at the same time. Users can play multicast videos from either the system's Admin Portal or User Portal.

Multicast of a Live Streaming

Users can start a multicast from the live streaming list. The system supports up to 100 concurrent multicast channels.

- VoD archive multicast is not supported.
- Streaming format is defined in meeting templates. For more information, see To define a recording template.

To start a multicast (when multicast is disabled):

1. Create a recording template with **Enable Multicast** selected.
2. Configure **Multicast TTL** from recording template.
3. Create a VRR with the configured recording template.
4. Start a live streaming with the VRR, and multicast starts at the same time.

To view a multicast streaming:

1. Click **Live Streaming**.
2 Select a live streaming and click Multicast Detail.
3 Click Play.
The media file is played in a new window.

- If there are MP4 and WMV streams, there would be two multicasts for the two stream types.
- If there are two bitrate streams, center will choose the higher bitrate stream to do multicast;
- You can view multicasts from either Admin or User Portal.

Certificate Management

X.509 certificates are a security technology that assists networked computers in determining whether to trust each other. The RealPresence Capture Server system supports using X.509 certificates (version 3 or earlier) for authenticating the network connections. Once a certificate is purchased and installed in the RealPresence Capture Server system, it may be used for the following connections:

- Web server (TLS)
- Microsoft Active Directory server (LDAPS)
- SIP recording (TLS)
- FTP Server (FTPS)

Install the Certificate in the System

Certificates and certificate chains are a security technology that allows networked computers to determine whether to trust each other.

By default, to support encrypted communications and establish a minimal level of trust, the system includes a default key and self-signed certificate.

However, to implement a full certificate chain to a root certificate authority (CA), the system requires both a root CA certificate and an identity server certificate signed by the root CA. Therefore, at some time you must request these certificates from your CA.

Install certificates on the RealPresence Capture Server system in Admin Portal

1 Install your chosen certificate authority’s public certificate, if necessary, so that the RealPresence Capture Server system trusts that certificate authority.
2 Create a certificate signing request to submit to the certificate authority.
3 Install a public certificate signed by your certificate authority that identifies the RealPresence Capture Server system.

The RealPresence Capture Server system accepts the following types of certificate chains or single certificates:

Certificate Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pem</td>
<td>Privacy Enhanced Mail, base64 encoded DER certificate, enclosed between &quot;-----BEGIN CERTIFICATE-----&quot; and &quot;-----END CERTIFICATE-----&quot;.</td>
</tr>
</tbody>
</table>
Install a Certificate Authority’s Certificate

You must install a certificate authority's certificate if you don't obtain a certificate chain that includes a signed certificate for the RealPresence Capture Server system, your certificate authority’s public certificate, and any intermediate certificates.

The certificate must be either a single X.509 certificate or a PKCS#7 certificate chain. If it is ASCII text, it's in PEM format, and starts with the text -----BEGIN CERTIFICATE-----.

To install a certificate for a trusted root CA:

1. Go to Configuration > Certificate Management.
2. If you are using a certificate authority that is not listed, obtain a copy of your certificate authority’s public certificate.
3. Select Install Certificates.
4. Do one of the followings:
   - Click Upload Certificate and click Add to browse to the certificate. Upload the selected certificate. Enter your password if necessary.
   - Copy the certificate text, and then click Paste certificate to paste it into the text box.
5. Click OK. If the certificate can be verified, the system installs it.

Create a Certificate Signing Request

This procedure creates a CSR (certificate signing request) that you can submit to your chosen certificate authority.

Creating a new CSR overwrites the existing pending CSR, if any.

To create a certificate signing request:

1. Go to Configuration > Certificate Management.
2. Select Issue Signing Request.
3 Enter certificate information:

Certificate Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>Specify the name of the system.</td>
</tr>
<tr>
<td>Organizational unit (OU)</td>
<td>Specify the business unit defined by your organization (Optional). Use a</td>
</tr>
<tr>
<td></td>
<td>comma(,) to separate several business units.</td>
</tr>
<tr>
<td>Organization</td>
<td>Specify your organization’s name (Optional).</td>
</tr>
<tr>
<td>City or locality (L)</td>
<td>Specify the city where your organization is located (Optional).</td>
</tr>
<tr>
<td>State (ST)</td>
<td>Specify the state or province where your organization is located (Optional).</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Specify your two-character country code.</td>
</tr>
</tbody>
</table>

4 Click OK.

The Certificate Signing Request dialog box displays the encoded request.

5 Copy the entire contents of the Encoded Request box and submit it to your certificate authority. Be sure to include the text -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----.

Depending on the certificate authority, your CSR may be submitted by pasting it into a web page.

6 Click OK.

When your request has been processed, your certificate authority sends you a signed public certificate for your RealPresence Capture Server system. Some certificate authorities also send intermediate certificates or its root certificates.

The certificate authority might send you the certificate as e-mail text, an e-mail attachment, or content on a secure web page.

Refer to To install a certificate for a trusted root CA:to install a certificate.

View Certificate Details

You can review installed certificate details.

To view the certificate details:

1 Go to Configuration > Certificate Management.

2 Click Display Details.

Certificate Details

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Info</td>
<td>States the purpose and alias of the certificate.</td>
</tr>
<tr>
<td>Issue To</td>
<td>States the entity to which the certificate was issued and the certificate serial number.</td>
</tr>
<tr>
<td>Issue By</td>
<td>States the issuer.</td>
</tr>
</tbody>
</table>
Remove a Certificate
You can remove installed certificates.

A certificate cannot be removed when it is the only private certificate which can be used as web service certificate in the system.

To remove a certificate:
1. Go to Configuration > Certificate Management.
2. Highlight the certificate you want to remove.
3. Click Delete.

Client Certification
If client certificate validation is enabled in the system, other systems can connect to the RealPresence Capture Server system only if they present a client certificate issued by a CA that the system trusts.

Enable the client certificate validation only in one of the following situations:

- Your network has implemented a complete PKI (Public Key Infrastructure) system, including a CA server, client software, and the appropriate operational procedures. Client hardware, tokens, and smartcards are optional.
- The CA's public certificate is installed in the RealPresence Capture Server system so that it trusts the CA.
- All authorized users’ systems, including yours, have a client certificate signed by the CA that authenticates them to the RealPresence Capture Server system.

To enable the client certificate validation:
1. Go to Configuration > Certificate Management.
2. Tick Enable web client certificate validation.
3. Click OK. The system restarts to apply your changes.

Use OCSP to Obtain Revocation Status
You can enable OCSP (Online Certificate Status Protocol) to obtain the revocation status of a certificate presented to the system.

If the certificate includes an AIA extension, the system has the information needed to configure OCSP for obtaining revocation status.
To configure OCSP:
1. Go to **Configuration > Certificate Management**.
2. Select **Enable OCSP**.
3. Click **OK**. The system restarts to apply your changes.

You need to check **Enable web client certificate validation** firstly for OCSP to take effect.

Use HTTP protocol to access website
In addition to HTTPS, you can now access the website using HTTP protocol.

To enable HTTP protocol for server website:
1. Go to **Configuration > Certificate Management**.
2. Select **Enable HTTP protocol for Server Website** check box under **Client Certificate**.
3. Click **OK**.

Configure QoS
QoS (Quality of Service) is very important in transmission of high-bandwidth audio and video data. You can use QoS to test and guarantee the following settings:
- Average packet delay
- Delay variation (jitter)
- Error rate

To specify QoS parameters:
1. Go to **Configuration > QoS**.
2. Configure the following settings:

QoS parameters
3 Click **OK**. The server restarts to apply your changes.

QoS settings applies to SIP and H.323 calls only, it does not apply to streaming.

### Configure SNMP

Your system provides a standard SNMP (Simple Network Management Protocol) interface which supports SNMP version 1, version 2, and version 3 queries with confidentiality, authentication, and integrity functions.
conforming to SNMP MIB. The interface uses a common MIB, making it interoperable with Polycom CMA, DMA, and RMX systems.

- Available configurable options vary with the SNMP agent version and security level selected.
- RealPresence Capture Server does not support SNMP trap.

**To configure SNMP settings:**

1. Click **Configuration > SNMP**.
2. Select **Enable SNMP**.
   
   SNMP is disabled by default.
3. Configure the following agent parameters:

### SNMP Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve MIB Files</td>
<td>Retrieve MIB file to your computer.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Specify the name of this RealPresence Capture Server agent.</td>
</tr>
<tr>
<td>Contact Country</td>
<td>Specify the contact country for this RealPresence Capture Server.</td>
</tr>
<tr>
<td>Contact Person</td>
<td>Specify a contact person for this RealPresence Capture Server.</td>
</tr>
<tr>
<td>SNMP Agent Version</td>
<td>Specify the SNMP Agent version.</td>
</tr>
</tbody>
</table>

4. Configure the following security settings:

### Security Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepted Host Community Name</td>
<td>Specify the community name that the host belongs to.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specify the user name that will be used to log in over the <strong>Authentication Protocol</strong>.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>Specify the type of encryption to use when connecting with this user:</td>
</tr>
<tr>
<td></td>
<td>• <strong>MD5</strong>: Message Digest 5</td>
</tr>
<tr>
<td></td>
<td>• <strong>SHA</strong>: Secure Hash Algorithm</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>Specify the password that will be used to log in over the <strong>Authentication Protocol</strong>.</td>
</tr>
</tbody>
</table>

**Note:** A valid password contains 8-64 characters, and not include these characters: &,'",<,>,%,:,+,=
Notice about Using Polycom SNMP MIB Files

Besides standard SNMP MIB files, RealPresence Capture Server also provides two proprietary MIB files:

- POLYCOM-BASE-MIB.mib
- POLYCOM-REAL-PRESENCE-MONITORING-MIB.mib

To use these Polycom MIB files, please first import the file POLYCOM-BASE-MIB.mib, then POLYCOM-REAL-PRESENCE-MONITORING-MIB.mib. Otherwise, the Polycom MIB files cannot be correctly compiled.

All RealPresence Capture Server MIB files can be downloaded from the Admin Interface Configuration > SNMP > Retrieve MIB Files.

Diagnostics

You can use Ping to verify that the RealPresence Capture Server system can communicate with another node in the network.

To run Ping on the RealPresence Capture Server system:

1. Go to Configuration > Diagnostics.
2. Enter an IP Address or Host Name and click Ping.
3. You will see the ping response shown in the ping result.

Active Directory

The Polycom RealPresence Capture Server system supports integration with a single Active Directory server.

After the integration, users in the Active Directory domain can access the Admin Portal or User Portal of the Polycom RealPresence Capture Server system directly as ordinary users without needing to be registered directly in the Capture Server system user database.

To configure an Active Directory server

1. Go to Configuration > Active Directory.
2. Configure the following settings:
When the RealPresence Capture Server system is connected to the Active Directory server, **Active Directory Status** on the page displays **Connected**.

If the system is configured with an Active Directory server, users defined on the Active Directory can log in to the Polycom RealPresence Capture Server system as ordinary users. When logging in to the Polycom RealPresence Capture Server system’s Admin Portal using an existing domain user, the user gets only ordinary user permissions.

### Password Settings

Go to **Configuration > Password Settings** you can manage your password, learn how to change the security policies that control what kind of password you use and how often you have to change it.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Active Directory</td>
<td>Specify whether to enable Active Directory functionality for this system.</td>
</tr>
<tr>
<td>Active Directory Address</td>
<td>Set the IP address or domain name of the Active Directory server to be integrated. Note: If you set a domain name, make sure you have already set a DNS server address that can resolve this domain name in <strong>Configuration &gt; IP Settings</strong>.</td>
</tr>
<tr>
<td>Active Directory Port</td>
<td>Specify the port number for the Active Directory, the default value is 636.</td>
</tr>
<tr>
<td>Active Directory User</td>
<td>Set the user name that will be used by the Polycom Capture Server system to access resources on the Active Directory server.</td>
</tr>
<tr>
<td>Active Directory Password</td>
<td>Set the user password that will be used by the Polycom Capture Server system to access resources on the Active Directory server.</td>
</tr>
<tr>
<td>Active Directory Base DN</td>
<td>Can be used to restrict the Capture Server system to work with a subset of the Active Directory (such as one tree of multiple trees, a subtree, or a domain). Leave the default setting, All Domains, initially.</td>
</tr>
<tr>
<td>Enable SSL Connection</td>
<td>Specify whether to enable SSL encryption for the communication between the RealPresence Capture Server system and the AD server.</td>
</tr>
<tr>
<td>Synchronize AD Time Point</td>
<td>Specify when to synchronize AD data on a daily basis.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the Active Directory server is reachable.</td>
</tr>
</tbody>
</table>

3  **Click OK**

When the RealPresence Capture Server system is connected to the Active Directory server, **Active Directory Status** on the page displays **Connected**.
## System Configuration

<table>
<thead>
<tr>
<th>Password Management</th>
<th>Password Expired Warning Period</th>
<th>Specify how far in advance the system displays a warning that the password will soon expire, if a maximum password age is set. Default: 10 (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximum Password Age</td>
<td>Specify the maximum number of days that can pass before the password must be changed. Default: 90 (days)</td>
</tr>
<tr>
<td></td>
<td>Minimum Password Age</td>
<td>Specify the minimum number of days that must pass before the password can be changed. Default: 0</td>
</tr>
<tr>
<td></td>
<td>Reuse Number of Password</td>
<td>Specify the number of most recent passwords that cannot be reused. For example, if set to 2, the last two passwords cannot be reused. Default: 0</td>
</tr>
<tr>
<td>Password Complexity</td>
<td>Allow to contain or reverse User ID</td>
<td>Specify whether to allow a valid password to contain the same characters, in the same order or reversed, as the user name.</td>
</tr>
<tr>
<td></td>
<td>Minimum Password Length</td>
<td>Specify the minimum number of characters required for a valid password. Default: 1 (day)</td>
</tr>
<tr>
<td></td>
<td>Minimum Password Changed Characters</td>
<td>Specify the number of characters that must be different or in a different position in a new password. If this is set to 3, “123abc” can change to “345cde” but not to “234bcd”. Default: 0</td>
</tr>
<tr>
<td></td>
<td>Maximum Consecutive Repeated Characters</td>
<td>Specify the maximum number of consecutive repeated characters in a valid password. If this is set to 3, “aaa123” is a valid password but “aaaa123” is not. Default: 0</td>
</tr>
<tr>
<td></td>
<td>Minimum Upper Case</td>
<td>Specify the minimum number of uppercase characters required for a valid password. Default: 0</td>
</tr>
<tr>
<td></td>
<td>Minimum Lower Case</td>
<td>Specify the minimum number of lowercase characters required for a valid password. Default: 0</td>
</tr>
<tr>
<td></td>
<td>Minimum Numeric Characters</td>
<td>Specify the minimum number of numbers required for a valid password. Default: 0</td>
</tr>
<tr>
<td></td>
<td>Minimum Special Characters</td>
<td>Specify the minimum number of special characters required for a valid password. Supported characters include the characters displayed in the Special Characters Set field. Default: 0</td>
</tr>
</tbody>
</table>
UI Customization

You can personalize the system appearance, for example, set the IVR information and set an e-mail address for your RealPresence Capture Server system.

Customize IVR Information

The RealPresence Capture Server system provides IVR (Interactive Voice Response) service. After the call to capture server is connected, the IVR will provide guide information to the user on the event happening at the capture server.

To customize the IVR information:

1. Go to Configuration > Customization.
2. Select the IVR information to be played and corresponding language option.
3. Click Upload.
   - The audio file to be uploaded must be in PCM format, and the sampling frequency must be 16KHz, 16bit, and mono.
4. Click Add, select the audio file and click Open.
5. Click OK.
## Default IVR Messages

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Text</th>
<th>When Played</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Welcome to conference record playback service.</td>
<td>When join the recording service where <strong>Start Recording Immediately</strong> is disabled.</td>
</tr>
<tr>
<td>Recording Started</td>
<td>Conference recording has started.</td>
<td>The conference recording has started.</td>
</tr>
<tr>
<td>Recording Stopped</td>
<td>The conference recording has ended.</td>
<td>The conference recording has ended.</td>
</tr>
<tr>
<td>Recording Paused</td>
<td>The conference recording is now paused.</td>
<td>The conference recording is paused.</td>
</tr>
<tr>
<td>Recording Resumed</td>
<td>The conference recording is now resumed.</td>
<td>The conference recording is resumed.</td>
</tr>
<tr>
<td>Disk Warning</td>
<td>You have exceeded your allocated disk space.</td>
<td>When there is not enough disk space to make recordings.</td>
</tr>
<tr>
<td>Call will be ended soon</td>
<td>The conference recording will end in another 10 minutes.</td>
<td>The conference recording is about to end in 10 minutes.</td>
</tr>
<tr>
<td>Playback Ended</td>
<td>Your playback has ended.</td>
<td>When the playback is ended.</td>
</tr>
<tr>
<td>Playback not allowed</td>
<td>You are not allowed to play back this archive.</td>
<td>You do not have permission to play back the archive after three failed attempts to input personal code.</td>
</tr>
<tr>
<td>Playback not processed</td>
<td>Sorry, your playback request can not be processed.</td>
<td>When play back an invalid archive.</td>
</tr>
<tr>
<td>Playback paused</td>
<td>Your playback is paused.</td>
<td>When the playback is paused.</td>
</tr>
<tr>
<td>Playback stopped</td>
<td>Your playback is stopped.</td>
<td>When the playback is stopped.</td>
</tr>
<tr>
<td>Playback session timeout</td>
<td>Your session has timed out, your call will hang up.</td>
<td>When play back an archive with enabled PIN code protection, if you do not input PIN code within 15 seconds or if the playback is paused for five minutes.</td>
</tr>
<tr>
<td>Input personal code</td>
<td>Please enter your personal code and then press the pound key.</td>
<td>When play back an archive under PIN code protection.</td>
</tr>
<tr>
<td>Invalid personal code</td>
<td>Invalid personal code, please try again.</td>
<td>When play back an archive with invalid PIN code.</td>
</tr>
</tbody>
</table>

## Customizing UI Logo

You can customize the logo displayed on both Admin Portal and User Portal.
To customize the Logo picture of the web Management interface:

1. Go to Configuration > Customization.
2. In the Logo area, click Change Logo > Add to select the picture to be uploaded.
3. The uploaded pictures must be in the *.png format, with 201 * 54 pixels.
4. Click Open > Upload.
5. Click OK.

Setup E-mail

You can set an e-mail address for your RealPresence Capture Server system. This is filled to “From” address in the e-mail the system sent out.

To set an e-mail address for the RealPresence Capture Server system:

1. Go to Configuration > Customization.
2. Configure the following settings:
   - **Admin Email Settings**
     - **Sender Email**: This is filled to “From” address in the email the system sent out.
     - **Frequency**: Select the period for automatic e-mail notification.
     - **Receiver Email**: The email is sent when there is administrative event occurs, like disk warning, alert, etc.
   - **Service Email Settings**
     - **Enable Email Notifications**: When enabled, you will receive e-mail notification when live streaming starts or archive is ready for VoD.

Portal Settings

- When using Polycom RealPresence Media Manager or other external portal to allow users to access live and on-demand streams, it is a best practice to redirect visitors from the Capture Server’s User Portal to the Media Manager (or 3rd party portal) home page.
- You can also manage session idle timeout and maximum number of login for both Admin and User Portal.
- You can select to show both internal and external live streaming URL.
### Portal Setting Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Redirect Settings</strong></td>
<td>Redirect users attempting to connect to User Portal (https://Capture_Server/portal) to the following URL: Enter a URL for visitors to redirect from Capture Server’s User Portal to the Media Manager (or 3rd party portal) home page.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the URL works.</td>
</tr>
<tr>
<td>Disable view permission of user portal for guest user</td>
<td>This is enabled by default and as a result, guest users on User Portal do not have view permission.</td>
</tr>
<tr>
<td><strong>Session Management</strong></td>
<td></td>
</tr>
<tr>
<td>Admin Portal</td>
<td>• <strong>Session Idle Timeout</strong>: specifies the number of minutes an Admin Portal session can be idle before the server cancels the session. The default value is 30.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Session Maximum Number Per Application</strong>: The maximum number of Admin Portal login. The default value is 200.</td>
</tr>
<tr>
<td>User Portal</td>
<td>• <strong>Session Idle Timeout</strong>: specifies the number of minutes a User Portal session can be idle before the server cancels the session. The default value is 30.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Session Maximum Number Per Application</strong>: The maximum number of User Portal login (including anonymous login). The default value is 3000.</td>
</tr>
<tr>
<td><strong>Streaming URL Settings</strong></td>
<td>Show both internal and external live streaming URL When selected, portal will show both external media server’s live stream URL and Capture Server’s native stream URL. By default this option is unchecked and only external media server’s live stream URL is shown.</td>
</tr>
</tbody>
</table>
Record and Playback

Configure Templates

A template is used to define a set of basic recording parameters, such as call rate of recording, video quality, whether to live stream and streaming rate. All Virtual Recording Rooms (VRR) are created based on templates. Changing parameters of a template may change the corresponding recording policies of the VRR using that template.

Configure Recording Templates

In this section you’ll learn how to configure recording templates, including how to view, define, edit or delete a recording template.

To view a recording template:

» Go to Template > Recording Templates.

To define a recording template:

1. Go to Template > Recording Templates.
2. Click Add.
3. Configure the following settings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Specify a unique name to identify this template.</td>
</tr>
<tr>
<td>Enable Live Streaming</td>
<td>Enable live streaming for the calls that use this template.</td>
</tr>
<tr>
<td>Disable Recording</td>
<td>This setting is available when Enable Live Streaming is selected. When this is selected, the call will be live streamed only, without recording.</td>
</tr>
<tr>
<td>Enable Multicast</td>
<td>Specify whether to enable multicast for the recording template.</td>
</tr>
<tr>
<td>Multicast TTL (available after multicast is enabled)</td>
<td>Choose from the drop-down list. The default TTL value is Auto -- Use System Setting. Note: The template value set here will override the system value.</td>
</tr>
<tr>
<td>Enable PIN</td>
<td>Specify whether to enable PIN code protection for the archive. If a PIN code is set, you must enter the correct PIN code to play the live streams or archives created using this VRR. After this option is selected, you must enter a PIN code consisting of 1-16 digits in PIN Code.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Call</td>
<td></td>
</tr>
<tr>
<td>Audio Only</td>
<td>Select this check box to define the recording for the call with this template has only audio capability, no matter the call rate negotiated.</td>
</tr>
<tr>
<td>Max Call Rate</td>
<td>Specify the maximum bandwidth that can be used by an endpoint or MCU to connect to the RealPresence Capture Server system for recording and live streaming.</td>
</tr>
<tr>
<td>Max Resolution</td>
<td>Specify the maximum resolution of people video that can be used to connect to the RealPresence Capture Server system for recording and live streaming.</td>
</tr>
<tr>
<td>Enable LPR</td>
<td>Once this function is selected, in case of packet loss during network transmission, it can effectively improve the decreased video quality caused by packet loss.</td>
</tr>
<tr>
<td>Indication Tone</td>
<td>Played to indicate that recording is ongoing, typically it is a very short beep with intervals between beeps, measured in second. This is enabled by default.</td>
</tr>
</tbody>
</table>
| Media Encryption Type | If the Capture Server is licensed for call encryption, this option specifies how AES (Advanced Encryption Standard) encryption is enabled and SIP connections:  
  • **Required For All Calls**: Enable the AES encryption for all H.323 and SIP calls, including video and audio only calls. This option requires the device to connect the system with AES enabled, otherwise, the connection cannot be set up.  
  • **When Available**: Both encrypted and non-encrypted undefined participants can connect to the same conferences, where encryption is the preferred setting.  
  • **Off**: Disable the AES encryption and SIP connections.  
  Note: The Media Encryption Type available here is consistent with that set under Set Recording Parameters. The encryption change is applied to new calls only and does not impact the archive. |
| Max Call Length | Specifies the maximum call length for recording or live streaming calls. The default option is **Auto** (When selected, the max call length setting will be the same as configured under Configuration > Call Settings).  
  Note: The template value set here will override the system value set under Configuration > Call Settings on Admin Portal. |
| Conference Layout (RMX 8.4 or higher) | Specify the people layout received and recorded from MCU. The **1x1** and **1x2** layout may give focus on the speaker of the conference in the recording.  
  • **Auto**: Automatic layout according to conference setting at RMX side to recording server.  
  • **1x1**: Single view to recording server.  
  • **1x2**: Dual view to recording server. |
| Archiving | |
### Record and Playback

<table>
<thead>
<tr>
<th>Start Recording Immediately</th>
<th>If this option is selected, the system immediately starts recording with this recording template. If deselected, you may need to manually start recording through the Admin Portal or the TV UI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Name Prefix</td>
<td>Specify the prefix of the output media archive name.</td>
</tr>
<tr>
<td><strong>Live Streaming (MP4)</strong></td>
<td></td>
</tr>
<tr>
<td>Enable H.264 High Profile for Live Streaming</td>
<td>Select this check box to enable the use of H.264 High Profile in Video Switching conferences.</td>
</tr>
<tr>
<td>Primary Streaming Rate (Kbps)</td>
<td>The default value is 1024 kbps. Once the streaming rate is set, you can define a name for this streaming.</td>
</tr>
<tr>
<td>Secondary Streaming Rate (Kbps)</td>
<td>The default value is Off. After a streaming rate is set here, you can define a name for this streaming.</td>
</tr>
<tr>
<td><strong>Layout</strong></td>
<td>Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Single window with small content (People 75%; Content 25%)</strong>: Displays dual stream in one window of which 75% is people video and 25% content video.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Single window with medium content in right (People 50%; Content 50%)</strong>: Displays dual stream in one window of which 50% is people video and 50% content video at the right side.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Single window with medium content in left (People 50%; Content 50%)</strong>: Displays dual stream in one window of which 50% is people video and 50% content video at the left side.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Single window with large content (People 25%; Content 75%)</strong>: Displays dual stream in one window of which 25% is people video and 75% content video.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Single window with people only (content not shown)</strong>: Displays people video only in one window with no content.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Single window with people or content (when content active)</strong>: When people and content videos coexist, content video takes priority, people video displays only when content is absent.</td>
</tr>
<tr>
<td><strong>Live Streaming (WMV)</strong></td>
<td></td>
</tr>
<tr>
<td>Primary Streaming Rate (Kbps)</td>
<td>The default value is Off. Once the streaming rate is set, you can define a name for this streaming.</td>
</tr>
</tbody>
</table>
### Secondary Streaming Rate (Kbps)
The default value is **Off**. Once the streaming rate is set, you can define a name for this streaming.

<table>
<thead>
<tr>
<th>Layout</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts:</td>
</tr>
<tr>
<td></td>
<td><strong>Single window with small content (People 75%; Content 25%)</strong>: Displays dual stream in one window of which 75% is people video and 25% content video.</td>
</tr>
<tr>
<td></td>
<td><strong>Single window with medium content in right (People 50%; Content 50%)</strong>: Displays dual stream in one window of which 50% is people video and 50% content video.</td>
</tr>
<tr>
<td></td>
<td><strong>Single window with medium content in left (People 50%; Content 50%)</strong>: Displays dual stream in one window of which 50% is people video and 50% content video.</td>
</tr>
<tr>
<td></td>
<td><strong>Single window with large content (People 25%; Content 75%)</strong>: Displays dual stream in one window of which 25% is people video and 75% content video.</td>
</tr>
<tr>
<td></td>
<td><strong>Single window with people only (content not shown)</strong>: Displays people video only in one window with no content.</td>
</tr>
<tr>
<td></td>
<td><strong>Single window with people or content (when content active)</strong>: When people and content videos coexist, content video takes priority, people video displays only when content is absent.</td>
</tr>
<tr>
<td></td>
<td><strong>Dual window for content (when inactive content, it is black)</strong>: The stream supports dual windows on Windows Media Player, one for people video, the other for content video, black screen displays when content is absent.</td>
</tr>
</tbody>
</table>

4 Click **OK**. You can click **Save As** to clone a new template with the same settings.

### To edit or delete a recording template:

1 Go to **Template > Recording Templates**.
2 Click the recording template you want to change.
3 Click **Edit** or **Delete**.

### Max Call Length
Maximum call length is used to restrict the call length for recording and streaming calls due to the following reasons:

- When record a meeting, the recording call may be endless (to RMX for example) and thus flood the disk for unused data.
- A recording longer than 8 hours is difficult to be offline-transcoded.
- An endless streaming only session will cost transcoding resource occupancy.

### To set max call length for recording and streaming calls

1 Go to **Template > Recording Templates**.
2 Select the recording template you want to change.
3  Click Edit.
4  Choose a value from the **Max Call Length** drop-down list.

   - The max call length is a guard timer used to automatically stop recording and disconnect to the recording client when timer times out. This is helpful to avoid flooding the disk if recording server fails to end the call after the recording event.
   - For a recording call (with or without live streaming), the default setting is 2 hours, range is 1-8 hours; for live streaming only calls, default setting is 8 hours and there is no limitation to max range.
   - When a call is approaching the max call length, an IVR message will be sent to user as a reminder.

To set max call length for streaming only calls:
1  Go to **Template > Recording Templates**.
2  Click the recording template you want to change.
3  Click **Edit**.
4  Select **Disable Recording**.
5  Clear **Auto** underneath **Max call Length**.
6  Enter your desired value.
   - Note: Input positive numbers and the value 0 indicates no limitation to this option.

**Configure Transcoding Templates**

In this section you’ll learn how to configure transcoding templates, including how to view, define, edit or delete a transcoding template, you can also learn how to replicate transcoding templates for external media servers.

To define a transcoding template:
1  Go to **Template > Transcoding Templates**.
2  Click **Add**.
3  Configure the following settings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>Specify a unique name to identify this template.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Specify the output media file format.</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>Specify the output media file bitrate.</td>
</tr>
<tr>
<td>Video Type</td>
<td>The video protocol used by the archive.</td>
</tr>
<tr>
<td>Frame Rate</td>
<td>Specify the media frame rate.</td>
</tr>
<tr>
<td>Max Resolution</td>
<td>Specify the maximum transcoding resolution.</td>
</tr>
</tbody>
</table>
You can click **Save As** to clone a new template with the same settings.
You can find some preconfigured templates for iOS and Android as follows:

**Preconfigured Templates for iOS**

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Resolution</th>
<th>Frame Rate</th>
<th>Bitrate</th>
<th>Aspect Ratio</th>
<th>Device</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iphone_M_2</td>
<td>640*480</td>
<td>30</td>
<td>1296</td>
<td>4:3</td>
<td>iPhone4 &amp; above</td>
<td>Baseline</td>
</tr>
<tr>
<td>Iphone_S_2</td>
<td>480*360</td>
<td>15</td>
<td>464</td>
<td>4:3</td>
<td>iPhone4 &amp; above</td>
<td>Baseline</td>
</tr>
<tr>
<td>Ipad_L</td>
<td>1024*768</td>
<td>30</td>
<td>1M</td>
<td>16:9</td>
<td>iPad 2, iPad mini</td>
<td>Baseline</td>
</tr>
<tr>
<td>Iphone_M_1</td>
<td>640*360</td>
<td>30</td>
<td>664</td>
<td>16:9</td>
<td>iPhone4 &amp; above</td>
<td>Baseline</td>
</tr>
<tr>
<td>Ipad_H</td>
<td>1920*1080</td>
<td>30</td>
<td>1.7M</td>
<td>16:9</td>
<td>New iPad, iPad Retina Display</td>
<td>High Profile</td>
</tr>
<tr>
<td>Iphone_S_1</td>
<td>480*270</td>
<td>15</td>
<td>464</td>
<td>16:9</td>
<td>iPhone4 &amp; above</td>
<td>Baseline</td>
</tr>
</tbody>
</table>

**Preconfigured Templates for Android**

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Resolution</th>
<th>Frame Rate</th>
<th>Bitrate (Kbps)</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD_H</td>
<td>480*360</td>
<td>30</td>
<td>500</td>
<td>Baseline</td>
</tr>
<tr>
<td>SD_L</td>
<td>176*144</td>
<td>12</td>
<td>56</td>
<td>Baseline</td>
</tr>
<tr>
<td>HD</td>
<td>1280*720</td>
<td>30</td>
<td>2M</td>
<td>Baseline</td>
</tr>
</tbody>
</table>

**To view a transcoding template:**

» Go to Template > Transcoding Templates.

**To configure a transcoding template for IIS media server:**

1. Go to Template > Transcoding Templates.
2. Click Add.
3. Select ISM for Media Type.
4. Select the IIS media server you configured in Transfer to Media Server field.
To configure a transcoding template for WOWZA media server:

1. Go to Template > Transcoding Templates.
2. Click Add.
3. Select MP4 for Media Type.
4. Select the WOWZA media server you configured in Transfer to Media Server field.

To edit or delete a transcoding template:

1. Go to Template > Transcoding Templates.
2. Click the transcoding template you want to change.
3. Click Edit or Delete.

Configure VRRs

A VRR defines recording parameters. You can create a VRR basing on recording templates. A VRR is identified by digits, and you can directly start recording using a specified VRR by adding the VRR number to the dial-in number.

A default VRR, named DefaultVRR, is built in the system. When an endpoint or MCU tries to connect by dialing the RealPresence Capture Server without VRR number specified, default VRR parameters are used. You can modify the default VRR but cannot delete it.

To define a VRR:

1. Go to Template > VRRs.
2. Click Add.
3. Configure the following settings (* indicates mandatory parameters).

VRR Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRR Name</td>
<td>Specify a unique name to identify the VRR. You can also use the default name generated by the system.</td>
</tr>
<tr>
<td>VRR Number</td>
<td>Specify a number to identify the VRR. You can directly dial the VRR to record by adding the VRR number when dialing the RealPresence Capture Server system. The number you entered must be unique and comprised of 4-8 digits. You can also use the number automatically generated by the system. Note: The initial digit of the VRR number cannot be zero.</td>
</tr>
<tr>
<td>Description</td>
<td>If necessary, you can enter additional VRR information, such as the owner and usage, in order to improve identification and classification management when there are many VRRs.</td>
</tr>
<tr>
<td>Recording Template</td>
<td>Specify the recording template. The template defines the basic recording link parameters.</td>
</tr>
</tbody>
</table>
Record and Playback

Transcoding Template
After recording is done, the system will do offline transcoding according to transcoding templates configured here. Multiple offline transcoding outputs are allowed.

Note: Only qualified transcoding template will apply. If the template parameters is higher than recorded raw parameters, then the template will be ignored. For example, if recording raw resolution (e.g. 4CIF) is less than transcoding template (e.g. 720p), then this transcoding template will be ignored.

Live Streaming Server
You can check configured live streaming server information including publish point template, stream alias, and streaming list.

Email Address (separated by ‘,’)
Once the live streaming is started or the VRR recorded video has completed its format conversion and is ready for viewing, the system sends an e-mail message to the address set here.

4 Click OK.

You can click Save As to clone a VRR with the same settings.

To add publishing points for external media servers:

1 Go to Template > VRRs.
2 Select a VRR and click Edit.
3 Click Add, select a live streaming server you configured.
4 Enter values in the Publish Point Template field.
5 Fill in an alias for this stream.
6 Select a live streaming bitrate.
7 Click .
   Always click Save before clicking OK; otherwise the entered data will be lost.
8 Click OK.

To edit or delete a VRR:

1 Go to Template > VRRs.
2 Click the VRR entry you want to edit or delete.
3 Click Edit or Delete.

Start a Recording

You can start recording in RealPresence Capture Server using one of the following methods:

- Call from RealPresence Capture Server to an interoperable endpoint from Admin Portal.
- Call from RealPresence Capture Server to an interoperable endpoint from User Portal
- Call RealPresence Capture Server from an interoperable endpoint.
- Start a recording from Polycom RMX system via recording link.
• Schedule a meeting on RealPresence Media Manager and connect the RealPresence Capture Server to an endpoint.

To start a recording from the Admin Portal:

1. Access Capture Server admin portal by its IP address or host domain name from a compatible browser.
2. Enter the user name and password to log in to the system.
3. Go to Home. In the Signaling Connection area, click Dial out to record.
4. Configure the following settings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Address            | Specify the calling address. The system supports entering the calling address with an extended service number in the address box. If you call a H.323 system, you can dial out to endpoints by entering the numbers in the following formats:  
  • [far end E.164 prefix] - Use when every system has registered to a gatekeeper. For example, if a far end system E.164 prefix is 9988.  
  • [Far End H.323 ID] - Use when every system has registered to a gatekeeper. For example, if a far end system H.323 ID is CS9988.  
  • [Far End IP Address] - Use when a system has not been registered to a gatekeeper. For example, if a far end system IP address is 172.22.33.44. |
| Signal             | Set the H.323 or SIP network type for the system to place a call. Your choice depends on the call type used by the peer device. |
| VRR Name           | Click Select to select a virtual recording room (VRR). You can use the built-in default VRR, or one you have created. A VRR defines recording policies. For more information, refer to Configure VRRs. |
| Event Name         | Specify a unique name for this event. |
| Max Call Rate (Kbps) | Display the maximum call rate specified in VRR |

5. Click OK.

Unlike administrators, normal users can only view and manage calls started by themselves.

Dial in from Endpoint

You can start recording by dialing RealPresence Capture Server or dial in to a VRR directly to start recording.
To start recording by dialing RealPresence Capture Server:

» Enter the E.164 prefix or H.323 ID or SIP URL of Real Presence Capture Server on the user interface of an interoperable endpoint, for example, from remote control of HDX or Group Series.

If your system or endpoint is not registered to the gatekeeper or to a SIP server, call the system IP address instead.

You can also dial in to a VRR directly to start recording by dialing one of the following:

For H.323 calls

● [RealPresence Capture Server IP]##[VRR number]
  For example, if the RealPresence Capture Server IP is 11.12.13.14, and the VRR number is 4096, dial 11.12.13.14##4096.

● [RealPresence Capture Server E.164 prefix][VRR number]
  For example, if the RealPresence Capture Server E.164 prefix number is 8888, and the VRR number is 4096, dial 88884096.

For SIP calls

● [VRR number]@[RealPresence Capture Server IP]
  For example, if the RealPresence Capture Server IP is 11.12.13.14, and the VRR number is 4096, dial 4096@11.12.13.14.

● [SIP peer prefix][VRR number]
  If the system has been registered to a SIP server, the SIP server should configure CaptureServer as a SIP peer. For example, if the SIP peer prefix of the Polycom RealPresence Capture Server system is 8888 and the VRR number is 4096, the dial string should be 88884096.

Record from RMX via Recording Link

Capture Server can automatically record, or automatic record and stream, when RealPresence Collaboration Server (RMX Series) is configured with a Capture Server Recording Link has enable in RMX Conference Profile. Refer to the Collaboration Server (RMX Series) Getting Started Guide and Administrator’s Guide.

Change Conference Layout for RMX Hosted Calls

Once the Capture Server Recording Link is enabled on RealPresence Collaboration Server system (version 8.4 or higher), a user dials into a conference hosted on RealPresence Collaboration Server, the layout can be changed once Capture Server is connected when configured with SIP calls only.

To set conference layout type in a recording template

1. Go to Template > Recording Templates.
2. Select a recording template you want to edit.
3. Click Edit.
4. Choose from the Conference Layout drop-down list:
   - AUTO: Automatic layout according to conference setting at RMX side to recording server
   - 1x1: Single view to recording server.
To change conference layout type for an ongoing call

1. On Capture Server Admin Portal, go to Signaling Connection and click .
2. Choose from the following layouts:
   - Auto: Automatic layout according to conference setting at RMX side to recording server.
   - 1x1: Single view to recording server.
   - 1x2: Dual view to recording server.

When an endpoint or MCU tries to connect by directly dialing the IP address or E.164 prefix of the RealPresence Capture Server system, the default VRR parameters are used to record. You can directly start recording using recording parameters defined in a VRR by adding the VRR number to the dial-in number.

If the RealPresence Capture Server system is configured in connection with a Polycom RMX series system through the recording link, you can specify the VRR to be used by adding the VRR number in the Recording Link field on the Polycom RMX system. For more information, refer to the Polycom RMX system Administrator’s Guide.

For prefix+VRR format, you need to add SIP Peer to Polycom DMA server, for details, refer to the Polycom DMA server’s Administrator’s Guide.

With the newly added Annex-O support, you can start recording by dialing one of the following:

- For incoming calls to Capture Server, the dial-in number is [VRR number]@[RealPresence Capture Server IP address].
- If you call from RealPresence Capture Server to an interoperable endpoint such as Polycom HDX Series system, the dial-out number is [RealPresence Capture Server E.164 suffix]@[HDX IP Address] or [RealPresence Capture Server H.323 ID]@[HDX IP Address]
- If you call from RealPresence Capture Server to a MCU, the dial-out number is [Conference ID]@[RMX IP Address]

Point-to-point Recording

Point-to-point recording allows a user to dial out to two endpoints from the Capture Server Admin Portal or User Portal, and record the two sites into same recording file.

To start point-to-point recording from Admin Portal

1. In the address line, enter the system’s IP address in this format: https://<system IP address>/admin.
2. Enter the user name and password to log in to the system.
3. Go to Home or Call. In the Signaling Connection area, click 2 Sites Recording.
4. Enter the addresses of the two H.323 endpoint participants.
5. Click OK.
Video Call Playback

This section introduces how to play back video files for both dial-in and dial-out calls.

Video Call Play Back when Dialing in from Endpoint

You can play back recorded media archives stored in RealPresence Capture Server using Quick Code. A quick code is generated automatically for every archive after the system completes a recording.

To view the quick code of an archive from Admin Portal

1. Go to Media > Archives.
2. The quick code is displayed in the Quick Code column.

To edit the quick code of an archive:

1. Go to Media > Archives.
2. Select an archive.
3. Click Edit.
4. Edit the quick code in Quick Code text filed.
5. Click OK.

To play back archives using the quick code:

» Dial using one of the following formats:

- **H.323:**
  - If the system has been registered to a gatekeeper, dial [Capture Server E.164 prefix][Quick Code]
  - For example, if the E.164 prefix of the Polycom RealPresence Capture Server system is 1234 and the quick code of the file to be played back is 0123456, dial 12340123456

For now it only available in H.323 point-to-point calls.
For point-to-point recording from User Portal, refer to To start point-to-point recording from User Portal

If you need to view the quick code of an archive from User Portal, log in to the User Portal firstly, the quick code is displayed beneath the archive names.

A quick code consists of 7 digits that start with the number 0. If the archive has multiple episodes, you can append the two-digit episode index to the seven-digit quick code in your dial string.
If the system has not been registered to a gatekeeper, dial [RSS IP address]##[Quick Code]
For example, if the IP address of the Polycom RealPresence Capture Server system is 10.1.2.3 and the quick code of the file to be played back is 0123456, dial 10.1.2.3##0123456.

**SIP:**

- If the system has been registered to a SIP server, the SIP server should configure CaptureServer as a SIP peer, dial [SIP Peer Prefix][Quick code].
  For example, if the SIP peer prefix of the Polycom RealPresence Capture Server system is 1234 and the quick code of the file to be played back is 0123456, dial 12340123456.
- If the system has not been registered to a SIP server, dial [Quick Code]@[RSS IP address]
  For example, if the IP address of the Polycom RealPresence Capture Server system is 10.1.2.3 and the quick code of the file to be played back is 0123456, dial 0123456@10.1.2.3.

If you want to play back the second episode of the archive, you can replace the quick code in above dial string by appending episode index, such as replace 0123456@10.1.2.3 with 012345602@10.1.2.3.

- If no press on your part, it will begin playing the next episode automatically 30 seconds after the end of the previous one.
- Once the archive playback is completed, Capture Server will drop from the multipoint call within five minutes if no command is given.
- Capture Server will terminate the call five minutes after the playback is paused.
- If the capacity supports 40 recordings only, the Quick Code playback function is not supported.

### Video Call Playback when Dialing out from Capture Server

**RMX Playback (RMX 8.5 or higher)**

If the Capture Server system dials into a conference hosted on RealPresence Collaboration Server, the layout can be changed once Capture Server is connected when configured with SIP calls only.

**To start a playback call:**

1. On Capture Server Admin Portal, go to Media > Archives.
2. Select an archive and click Playback.
3. Fill in the IP address.
4. Choose a signaling protocol.
5. Choose from the following layouts:
   - **Auto:** Automatic layout according to conference setting at RMX side to recording server
   - **Lecture:** The playback video is viewed in full screen by all conference participants.
6. Choose an episode from the drop-down list.
7. Click OK.

- Once the archive playback is completed, Capture Server will drop from the multipoint call within five minutes if no command is given.
- Capture Server will terminate the call five minutes after the playback is paused.
When video call play back to RMX, the conference layout type can be changed. You can reuse the current overview.

**To change conference layout type for an ongoing call**

1. Go to **Signaling Connection** and click.
2. Choose from the following layouts:
   - **Auto**: Automatic layout according to conference setting at RMX side to recording server.
   - **Lecture**: The lecturer is viewed in full screen by all conference participants, while the audience is “time-switched” in the speaker’s view.

   It's for SIP calls only.
Live Streaming

The RealPresence Capture Server system supports live streaming of video sources, such as live video conference or dual stream sent by endpoints or MCUs with a highest resolution of 1080p and a maximum bandwidth of 4M. Those live streaming videos are saved in the system.

Live streaming supports dual streaming rates; this allows you to choose the appropriate bandwidth to view video based on your network condition.

Multi-bitrate Live Streaming

If the recording template is configured, the Capture Server system could send a specific resolution live stream to low bandwidth sites and a higher quality resolution live stream to high bandwidth sites without creating separate video broadcasts.

To live stream meetings to an external server, follow these steps:

1. Configure the external media server on the RealPresence Capture Server system and enable live streaming.
2. Configure a recording template that enables live streaming.
3. Configure a VRR that enables external media server.
4. Record a meeting using the VRR that has the external media server enabled.
   Refer to the following instructions to configure the external media servers to work with the RealPresence Capture Server system.

To configure live streams in recording template

1. Go to Template > Recording Templates.
2. Select a recording template.
3. Click Edit.
4. Select Enable Live Streaming.
5. Go to Live Streaming (MP4) and select Enable H.264 High Profile for Live Streaming.
6. Set the Primary Streaming Rate and Secondary Streaming Rate.
7. Go to Live Streaming (WMV) and configure relevant settings.
8. Click OK.

For configuration details, refer to table "Recording Template"
Start Live Streaming

Procedure for starting a live streaming is the same as the one for starting recording. For more information, see Start a Recording.

View Live Streaming Information

If live streaming is in progress on the system, the current live streaming list displays on the Live Streaming page. Go to Media > Live Streaming menu to enter the Live Streaming page.

The live streaming list displays live streaming summary, such as live streaming name, VRR number used, start time, live streaming detail and multicast detail.

View Live Streaming Video

When the system starts live streaming, you can view the video being live streamed in real time on the Live Streaming page.

To view live streaming in progress:

1. Go to Media > Live Streaming.
2. Select the live streaming content you want to view in the list, and then click ➤ in the Live Streaming Details area on the right side of the page. The system’s User Portal opens to play the video.

   If the live streaming content uses two different bandwidths, two Play buttons with their bandwidths appear in this area, and you may choose the appropriate bandwidth to play based on your network condition.

   You can also view live streaming links on Home and Call.

Configure External Media Servers

You can now stream live meetings and on demand meeting archives to leading 3rd party media servers, such as Wowza, IIS Media Service (Smooth Streaming only) and Windows Media Server.

Configure IIS or Wowza Media Server

You need to configure a Wowza or IIS media server and your RealPresence Capture Server to work with the server as well.

To configure IIS and WOWZA media servers:

1. Click IIS or WOWZA under Server.
2. Click Add.
3 Configure the following basic settings.

External Media Servers Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Specify the name of the external server.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Specify the IP or DNS of the external server you selected.</td>
</tr>
</tbody>
</table>
| Server Port                   | Specifies the port that the RealPresence Capture Server system uses to send the encoded MP4 live streams to the external server. Following are the default ports:  
  • IIS Media Server: 80  
  • Wowza Media Server: 1935  
  **Note**: Valid port values range from 1-65536. The port number must be the same as set in the corresponding external media server. If a firewall sits between the RealPresence Capture Server system and the external server, make sure that rules are set to allow the two-way communication between the RealPresence Capture Server system and the external server. |

4 Specify whether to select Enable Live. If enabled, also configure the following settings:

Enable Live Streaming

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Protocol (for WOWZA only)</td>
<td>Choose between RTSP Streaming and RTMP Streaming.</td>
</tr>
</tbody>
</table>
| Application Name              | Specify the name of the external media server’s application to be used for the live streaming.  
  **Note**: Contact the administrator of the external media server for the naming rule of the application name. |
| User Name                     | Specify the user name to access the external media server.                   |
| Password                      | Specify the password to access the external media server.                    |
| Test                          | Test whether the live streaming configurations work.                          |

Configure Windows Media Server

You need to configure a Windows media server and your RealPresence Capture Server to work with the server as well.

To configure Windows Media Server:

1 Click Windows Media Server under Server.
2 Click Add.
3 Configure the following basic settings.

**External Media Servers Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Specify the name of the external server.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Specify the IP or DNS of the external server you selected.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>The default value is 80.</td>
</tr>
<tr>
<td>RTSP Port</td>
<td>The default value is 554.</td>
</tr>
</tbody>
</table>

4 Specify whether to select **Enable Live**. If enabled, also configure the following settings:

**Enable Live Streaming**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Specify the user name to access the external media server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password to access the external media server.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the live streaming configurations work.</td>
</tr>
</tbody>
</table>

**Configure AKAMAI CDN**

You need to configure an AKAMAI media server and your RealPresence Capture Server to work with the server as well.

**To configure AKAMAI Media Server:**

1 Click **AKAMAI** under **Server**.
2 Click **Add**.
3 Configure the following basic settings.

**External Media Servers Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Name</td>
<td>The CONFIG NAME displayed on AKAMAI configuration page under PUBLISH &gt; Manage Streams.</td>
</tr>
<tr>
<td>Stream Name</td>
<td>The STREAM NAME displayed on AKAMAI configuration page under PUBLISH &gt; Manage Streams.</td>
</tr>
<tr>
<td>Stream Number</td>
<td>The STREAM ID displayed on AKAMAI configuration page under PUBLISH &gt; Manage Streams.</td>
</tr>
</tbody>
</table>
To add publishing points for external media servers:
1. Go to Template > VRRs.
2. Select a VRR and click Edit.
3. Click Add, select a live streaming server you configured.
4. Enter values in the Publish Point Template field.
5. Fill in an alias for this stream.
6. Select a live streaming bitrate.
7. Click Save. Always click Save before clicking OK; otherwise the entered data will be lost.
8. Click OK.

Pre-link Event

Sometimes for significant events like webcast or CEO meetings you may need to send meeting logistics beforehand, this feature provides pre-link URL for recording, live streaming and multicast live streaming events.

To create a pre-link event:
1. Go to Template > Events.
2. Click Add.
3  Configure the following settings (* indicates mandatory parameters).

### Pre-link Event Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Name</td>
<td>Specify a unique name for this event. A valid event name contains lowercase characters (a–z), uppercase characters (A–Z), numbers (0–9), space or multibyte characters.</td>
</tr>
<tr>
<td>Event Number</td>
<td>Specify a number to identify the event, you can also use the number automatically generated by the system. Note: The valid number ranges from 300-399.</td>
</tr>
<tr>
<td>VRR Name</td>
<td>Choose a VRR from the drop-down list.</td>
</tr>
<tr>
<td>URL Extension</td>
<td>Extension of the streaming URL, this is available after live streaming is enabled for the recording template in the selected VRR. Note: You need to enable live streaming in recording template. Valid extension contains lowercase characters (a–z), uppercase characters (A–Z), and numbers (0–9).</td>
</tr>
<tr>
<td>Multicast URL Extension</td>
<td>Extension of the multicast URL, this is available after multicast is enabled for the recording template in the selected VRR. Note: You need to enable multicast in recording template. Valid extension contains lowercase characters (a–z), uppercase characters (A–Z), and numbers (0–9).</td>
</tr>
<tr>
<td>Start Date</td>
<td>Which date the event will start. Note: The event cannot start automatically, the start date is for reference only.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Which time the event will start. Note: The event cannot start automatically, the start time is for reference only.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify additional related information.</td>
</tr>
<tr>
<td>Event Change Notification</td>
<td>When enabled, you receive e-mail notification once changes are made to the configured pre-link event settings.</td>
</tr>
<tr>
<td>Email Address (separated by ',')</td>
<td>Once changes are made to the configured pre-link event settings, the system sends an e-mail message to the address set here. Separate several addresses with comma (,).</td>
</tr>
</tbody>
</table>

4  Click OK.

You need to fill out either **URL Extension** or **Multicast URL Extension**, otherwise the pre-link event is created but the pre-link URL will not be generated.
Add event example

Add Event

To edit a pre-link event:
1. Go to Template > Events.
2. Select the event you want to change.
3. Click Edit.

To obtain the pre-link URL extension:
1. Go to Template > Events.
2. Select an event from the list.
3. Click Copy Prelink.
Copy prelink information

1. Go to Home.
2. In the Signaling Connection area, click Dial out to record.
3. Configure relevant settings. You need to select Event Name for the recording to start.
4. Click OK.

- If you click the URL before or after the event, there will be a pop-up message The stream is not available now.
- When the event starts, the player will refresh the URL and display the stream.
Media Management

You can archive your conferences and manage your archives.

Manage Archives

You can view all files recorded by the RealPresence Capture Server system in the Media > Archives page. An administrator can view, play back, delete, download, or re-transcode these media files.

View Archive Details

On the Media > Archives page, administrators can view a summary of each archive.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The ID for this archive.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the archive.</td>
</tr>
<tr>
<td>Duration</td>
<td>The duration of the archive.</td>
</tr>
<tr>
<td>Video Type</td>
<td>The video codec type used by the archive.</td>
</tr>
<tr>
<td>Audio Type</td>
<td>The audio codec type used by the archive.</td>
</tr>
<tr>
<td>Content Type</td>
<td>The content video type of the archive.</td>
</tr>
<tr>
<td>Key Words</td>
<td>The keywords for this archive.</td>
</tr>
<tr>
<td>Description</td>
<td>Additional user information.</td>
</tr>
</tbody>
</table>

Play Back and Download Archives

The RealPresence Capture Server system can transcode recorded videos into different formats, layouts and bit rates, including:

- **RAW**: RAW bit stream is automatically generated after the system completes the recording, also can be transcoded if transcoding template is configured.
  
  The RAW files are stored in a proprietary format. They are used as the source file to transcode other media formats. For detailed transcoding settings, refer to Configure Transcoding Templates.

- **MP4**: MP4 archives (Also known as H.264 streaming files) can be downloaded.
● **M4A**: M4A (audio only file) files can be downloaded to PCs, Macs, or to compatible digital media devices, but cannot be play backed from portals.

● **ISMV**: After the ISMV files are generated, they are uploaded to the IIS Media Server, and can be viewed from the User Portal.

   The ISMV files are generated only when the transcoding template is configured with IIS Media Server and the transcoding template is added in VRR.

● **WMV**: WMV files can be transcoded if transcoding template is configured. They can be downloaded to PCs or to compatible digital media devices.

**To play back archives through the Admin Portal:**

1. Go to Media > Archives.
2. Select the archive you want to play back.
3. Click ➔ and the User Portal opens to play the video.

   If the e-mail notification function has been enabled for the VRR that is used to record archives, the system sends you an e-mail notification automatically once all archives have been converted and are ready for web playback. For more information, see Configure VRRs.

**To download one or several archives from Archives page:**

1. Go to Media > Archives.
2. Select the archive you want to download.
3. Click Download.
4. Select one or several media types to download.
5. Click OK.

**To download one or several media files from Media Files page:**

1. Go to Media > Archives.
2. Select the archive you want to download.
3. Click Media Files.
4. Select one or several media files to download.
5. Click ∨.

**Manage Archives**

You can edit or delete archives recorded by your own archives that you are authorized to modify.

**To modify archive properties:**

1. Go to Media > Archives.
2. Double-click the archive entry you want to modify.
If you are authorized to modify the archive, you can modify following parameters:

### Archive Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name of the archive.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify additional related information.</td>
</tr>
<tr>
<td>Enable PIN</td>
<td>Specify whether to enable PIN code protection for the archive.</td>
</tr>
<tr>
<td>Key Words</td>
<td>Specify additional information related to the archive.</td>
</tr>
<tr>
<td>Quick Code</td>
<td>Generated automatically for every archive after the system completes a recording</td>
</tr>
</tbody>
</table>

If you want to change the list of users who can view or modify the archive, click the **Allowed Users/Groups** tab.

Choose an item (Users/Groups/AD Groups) from the drop-down list and click **Add**.

Click **OK**.

To delete one or several archive files:

1. Go to Media > Archives.
2. Select one or several archive files you want to delete.
3. Click **Delete**.
4. Click **OK** at the prompt message.

### Dynamic Archiving

You can view all media files included in an archive, create new media output formats on the fly, stop ongoing media file creation, or delete existing media files. You can also restart transcoding after you stop the transcoding, or when there is transcoding error.

To add new media files:

1. Go to Media > Archives.
2. In the archives list, select an archive.
3. Click **Media Files**.
4. Select one media file.
5. Click **Add**.
6. Select one or several transcoding templates.
7. Click **Add**, and then click **Close**.
To delete a media file:

1. Go to Media > Archives.
2. In the archives list, select an archive.
3. Click Media Files.
4. Click a media file to be deleted, and then click Delete.
5. Click OK, and then click Close.

Archives will be deleted permanently once you choose delete action on Admin Portal.

Transcoding Task Control

In this section you can learn how to view transcoding status, stop an ongoing transcoding, or restart a transcoding.

To view transcoding status:

1. Go to Media > Transcoding.
2. In the archives list, select an archive.
3. Click Media Files. Media files transcoding can have the following status:
   - Ready: The file can be played and downloaded.
   - Waiting: File waiting to be transcoded
   - Transcoding: File in transcoding.
   - Error: File with transcoding error.
   - Stopped: File creation stopped.
4. Click Close to exit the Media Files window.

To stop an ongoing transcoding:

1. Go to Media > Transcoding.
2. Click a media file of the status Transcoding or Waiting, and then click Stop-transcode.
3. Click OK, and then click Close.

You cannot stop transcoding files of the status Error or Stopped.
To restart a transcoding:

1. Go to Media > Transcoding.
2. Click a media file to be restarted, and then click Re-transcode.
3. Click OK, and then click Close.

You cannot restart transcoding for files of the status Transcoding or Waiting.
System Administration

System Upgrade and Fallback

You only can upgrade or downgrade RealPresence Capture Server between RealPresence Capture Server versions. Upgrading or downgrading between RealPresence Capture Server and Polycom RSS 4000 is not supported.

- You can upgrade your system from 1.7 to 1.8 directly. If your software version is older than version 1.7, you need to upgrade your system to 1.7 first, then upgrade your system to 1.8.
- After system upgrade from 1.7 to 1.8, you need to re-activate the system using an activation key.
- Before you upgrade or downgrade your system, you should always back up your settings and recordings. Polycom is not responsible for any user data loss during these operations.

To update your system software to the latest version:

1. Go to Admin > System Upgrade.
2. View the license info and agree to them.
3. Click Add and select the version 1.8 software upgrade package, then click Open.
4. When asked to confirm the action, click Yes. The system uploads the package and performs the upgrade automatically. This may take several minutes.
5. Upon completion of the upload, click Upgrade. The system restarts to apply changes.
6. Enter your administrator User ID and Password and then click Log In.
   To confirm that the system is upgraded, check the software version on the Product Activation page.

System Fallback

Before system upgrade, the system creates a restore point automatically and after system upgrade, you can restore both image data and system configuration settings that existed at the time the snapshot was created.

To fall back the image, configuration and IVR messages

1. Go to Admin > System Fallback.
2. Read the risk of system fallback and agree to it
3. Click Fallback Capture Server.
4 Click OK. The system restarts to apply the changes.

Fall back the system early as possible if you find it necessary after system upgrade, otherwise user data of the following operations will not be saved.

System Log Configuration

The logger utility is activated at the system startup and continually records system events. The log files generated by the utility contain the following information:

- Events occurred in system internal modules.
- Administrator activities.
- System login attempts.
- Operation errors.

All log files generated the day before are automatically compressed into a ZIP file named year-month-date.tar.gz at log maintenance window every day. The log maintenance window is usually the first hour from 00:00:00 system time every day. The log file storage is 30GB. You are prompted when the system reaches the storage limit. The system will delete the old logs to free the disk space at log maintenance window.

Configure Log Settings

You can change the system logging strategy, configure warning limit, and enable remote logging.

To configure the log settings:

1 Go to Admin > Log Settings.
2 Configure the following settings:
   - Logging Level: Specify the system logging level, which decides to what level system events should be written into the center/server.log file.
     - Info – logs all non-debug messages.
     - Debug – logs all messages.
     - Error – logs the fewest number of messages.
     - Warning – logs between error and Info messages.
   - Logger Warning Capacity: Specify the percentage of log file capacity used at which the system displays a warning on the dashboard.
   - Log retention period (days): Defines the number of days to keep log archives on server.
   - SysLog Server IP Configuration: To configure the IP settings of the SysLog server.
Log Management

The following table shows actions administrators and auditors can perform.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Refreshes the list and adds newly generated log files.</td>
</tr>
<tr>
<td>Download</td>
<td>Downloads the selected log file.</td>
</tr>
<tr>
<td>Download Today's logs</td>
<td>Downloads all the log files generated today.</td>
</tr>
</tbody>
</table>

To download log files:

1. Go to Admin > System Logs.
2. In the Log list, select the log to be saved.
3. Click Download.

Restart and Shut Down the System

You can shut down or restart your system.

Before unplugging RealPresence Capture Server, you need to shut down the server in Admin Portal.
If your RealPresence Capture Server does not restart after reboot or upgrade, you need to unplug your RealPresence Capture Server, wait for about five minutes, plug in your RealPresence Capture Server, and then reboot.

To restart the Capture Server system:

1. Go to Admin > Restart/Shutdown.
2. Read the risk of restart and click Restart Capture Server.
3. Click OK at the prompt message.

To shut down the Capture Server system:

1. Go to Admin > Restart/Shutdown.
2. Read the risk of shutdown and click Shutdown Capture Server.
3. Click OK at the prompt message.

Backup and Restore System Configuration

You can back up and save the system configuration of RealPresence Capture Server system to your local computer so you can restore the system configuration in case of necessary. Supported configurations include:

- Hard Disk Warning Threshold

Polycom, Inc. 84
● IP setting parameters
● System time
● Recording Settings
● Certificate, port and security policy
● Gatekeeper, SIP, and QoS Settings

To back up current system configuration:
1. Go to Admin > Config Backup/Restore.
   The configuration file will be stored on the local machine that the browser is running on.
2. Click Backup.

To restore the system configuration using the configuration file:
1. Go to Admin > Config Backup/Restore.
2. Click Add, select the .ppm file from local machine and click Open.
3. Click Upload.
4. Click Restore.
5. Confirm to restart the system.

Back Up and Restore Media Files
The RealPresence Capture Server system is able to backup media data to the FTP server in the network, and restore system user data to the selected media data snapshot (based on the time points generated in the backup). You can back up the entire media data. RealPresence Capture Server only uses passive mode FTP to transfer files.

Configure an FTP Server for Backup
Before backing up user data, you need to configure FTP server on the RealPresence Capture Server system first.

The RealPresence Capture Server system supports the following FTP servers:
- 3CDaemon
- FileZilla Server
- Serv-U
- Microsoft FTP7.x For IIS
- vsftpd

Back Up and Restore Archives
There are three ways to backup archives on the RealPresence Capture Server system to a FTP server:

- Automatic Archive: The frequency is less than 7 days and the start time can be configured with timezone info.
• **Automatic Media Backup**: This is always incremental backup, users can specify a **Frequency** of less than 7 Days and times are available in one-hour increments.

• **Manual Media Backup**: Includes full backup and incremental backup, it applies to both NFS and RAID storage.

**To automatically back up archives after call (Automatic Archive):**

1. Go to Admin > Data Backup/Restore.
2. Select **Automatic Archive** from **Backup type** dropdown list.
3. Configure the following settings for both FTP server and alternate FTP server.

**FTP Server Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>Enter the IP address of the FTP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port of the FTP server.</td>
</tr>
<tr>
<td>Media Backup Path</td>
<td>Specify the default FTP directory to save your media files.</td>
</tr>
<tr>
<td>User Name</td>
<td>Enter the account and password for login to the FTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Note: The registered FTP user should possess read-write permissions to user root directory.</td>
</tr>
<tr>
<td>Use Anonymous</td>
<td>When this is enabled, you can log in to the FTP server using anonymous account.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Set whether to enable SSL encryption for the communication between the RealPresence Capture Server system and FTP server. The system can only support implicit SSL FTP.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the FTP configurations work.</td>
</tr>
</tbody>
</table>

4. Finish **Alternate FTP Server Configuration** if needed.
5. Click **Update**.

Once this function is enabled, archives could be transferred to configured FTP server and removed from local disk after call, this is achieved automatically.

**To automatically back up media files (Automatic Media Backup):**

1. Go to Admin > Data Backup/Restore.
2. Select **Automatic Media Backup** from the **Backup type** dropdown list.
3. Configure the following settings:

**FTP Server Parameters**
To back up the archives manually (Manual Media Backup):

1. Go to Admin > Data Backup/Restore.
2. Select Manual Media Backup from the Backup type dropdown list.
3. Configure the following settings per information above.
4. Click Full backup or Increment backup.

You can see the backup status in Backup/Restore Status. The system archives are backed up to the configured FTP server.

To restore the archives:

1. Go to Admin > Data Backup/Restore > Restore.
2. Choose a restore point from the dropdown list.
3. Click Restore.
4. Confirm to restart the system.

Rebuild RAID

RealPresence Capture Server supports RAID 10 (RAID1 for 6/3 port license which is available in Chinese market). This appendix explains when you should rebuild RAID, how to replace failed hard disks, and how to rebuild RAID.

- Rebuild RAID Conditions
Replace a Hard Disk

Rebuild RAID

Rebuild RAID Conditions

RealPresence Capture Server supports RAID 10 (RAID1 for 6/3 port license which is available in Chinese market). Two TB hard disks are used as one RAID logical unit. It supports up to 4 (2 for 6/3 port license which is available in Chinese market) TB storage. Each hard disk is marked with a number as shown in the following illustration.

Hard Disk Number for RAID 1

![Hard Disk Number for RAID 1](image)

Hard Disk Number for RAID 10

![Hard Disk Number for RAID 10](image)

You can see the status of each hard disk on the Admin Portal. See Hardware Status for details. If the status of a hard disk is error, you need to remove this hard disk and order a new one.

- Shut down your RealPresence Capture Server before you change hard disks.
- RealPresence Capture Server does not support hot swapping.
- Contact your local Polycom representative to order a replacement hard disk.
After you use new hard disks, the system may need to rebuild RAID and data may be lost as shown in the following table.

**Rebuild RAID 1**

<table>
<thead>
<tr>
<th>User Case</th>
<th>Rebuild RAID?</th>
<th>Lost Data?</th>
<th>Does RealPresence Capture Server go back to work immediately?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace one hard disk.</td>
<td>No</td>
<td>No</td>
<td>Yes. After you replace the hard disk and reboot the system, the system only needs to reorganize the data on the new hard disk. The RAID status is Degraded (Recovering).</td>
</tr>
<tr>
<td>Replace two hard disks when RAID fails.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes. After you replace the hard disks and reboot the system, the system will go to the recovery mode. You need to rebuild RAID under the recovery mode manually, which takes 10 minutes. After rebuilding RAID, the system will go back to work. You lost all the previous data. The status of RAID is Normal (Resyncing). It takes about 4 to 5 hours to finish the resyncing process.</td>
</tr>
</tbody>
</table>

**Rebuild RAID 10**

<table>
<thead>
<tr>
<th>User Case</th>
<th>Rebuild RAID?</th>
<th>Lost Data?</th>
<th>Does RealPresence Capture Server go back to work immediately?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace one hard disk.</td>
<td>No</td>
<td>No</td>
<td>Yes. After you replace the hard disk and reboot the system, the system only needs to reorganize the data on the new hard disk. The RAID status is Degraded (Recovering).</td>
</tr>
<tr>
<td>Replace two hard disks when RAID is degraded.</td>
<td>No</td>
<td>No</td>
<td>Yes. After you replace the hard disks, RealPresence Capture Server will send an e-mail to remind you restart the system. After you reboot the system, the system only needs to reorganize the data on the new hard disk. The RAID status is Degraded (Recovering).</td>
</tr>
</tbody>
</table>
Replace a Hard Disk

If the status of a hard disk is error, you will see a hardware alert indicating failed hard disks after you log in to the Admin Portal. Polycom recommends that you to replace all failed hard disks.

**To replace a hard disk:**

1. Shut down your RealPresence Capture Server. See **Restart and Shut Down the System** for details.
2. Press the brown buckle on the front panel of RealPresence Capture Server as shown in the following illustration.

**Replace Hard Disk for RAID 1**
Replace Hard Disk for RAID 10

3. Pull out the hard disk.
4. Unscrew the three screws on both sides of the hard disk as shown next.

Unscrew Hard Disk

5. Replace the failed hard disk by screwing a new hard disk to the tray.
6. Insert the hard disk back to its slot.

Rebuild RAID

When one or more hard disks does not work, you will see a hardware alert indicating failed hard disks on the Admin Portal. You need to replace failed hard disks and reboot RealPresence Capture Server, the RAID status will change to Degraded or the system will go to the recovery mode in case of RAID failure. This always means that you need to rebuild RAID.

To rebuild RAID:
1. Replace failed hard disks. See Replace a Hard Disk.
2. Restart your RealPresence Capture Server. See Restart and Shut Down the System.
3. Connect a USB key to the Capture Server system and reboot to get to the recovery mode.
4. Enter your password to log in the recovery mode after the system is restarted. The default password is SUPPORT.
5. Check the RAID status under the recovery mode. Click Hardware Diagnose on the left, you will see the hardware status as shown in the following illustration. Only when the RAID status is FAILED, you need to rebuild RAID.
RAID Status

6 Select **Reset Raid Storage** on the left as shown next.

Rebuild RAID

7 Click Yes to rebuild RAID.

You will see all the detailed information in the **Server Status** panel. After the rebuilding RAID process done, you will see the message *format done* and the server status will returns to **IDLE** as show next.
Rebuild RAID Process

Server Status: IDLE

Begin to check RAID partition
online data are /dev/sdb /dev/sdc /dev/sdb /dev/sda, count is 4

clean /dev/sdb super block of raid md0 and container md126

clean /dev/sdc super block of raid md126 and container md127

clean /dev/sdb super block of raid md126 and container md127

clean /dev/sdc super block of raid md126 and container md127

mdadm --run /dev/md126 /dev/sdb /dev/sdc /dev/sdb -a /dev/sda -4

raid1dev/md0 created. Start to format...

format done

8. Click Reboot System. Your RealPresence Capture Server will go back to work.
System Indicators

When the system is running, indicators on the front panel indicate operating conditions of the system. The following table lists the indicators and their explanations.

System Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Panel Identifier</th>
<th>Status</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN 1 Activity Status Indicator</td>
<td>LAN 1 LED</td>
<td>Green</td>
<td>Network Connection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>No Network Connection</td>
</tr>
<tr>
<td>LAN 2 Activity Status Indicator</td>
<td>LAN 2 LED</td>
<td>Green</td>
<td>After the LAN 2 port is activated from Configuration &gt; IP Settings, the LED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>is green when there is network connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>No Network Connection</td>
</tr>
<tr>
<td>SSD Status Indicator</td>
<td>SSD LED</td>
<td>Orange</td>
<td>SSD Reading or Writing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>Hard Disk Idle</td>
</tr>
<tr>
<td>Power Status Indicator</td>
<td>Power LED</td>
<td>Green</td>
<td>System Power on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>System Power off</td>
</tr>
<tr>
<td>Power Failure Indicator</td>
<td>Power Failure LED</td>
<td>OFF</td>
<td>Power Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red</td>
<td>Power Supply Failure</td>
</tr>
<tr>
<td>Overheat and Fan Indicator</td>
<td>Overheat and Fan LED</td>
<td>Blinking Red (1 HZ)</td>
<td>Fan Failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking Red (0.25 HZ)</td>
<td>Power Failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Continuously Blinking Red</td>
<td>Overheat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>Normal</td>
</tr>
</tbody>
</table>
Manage Archives and Live Streams Using the User Portal

The RealPresence Capture Server provides User Portal for you to view live streaming, play back archives and dial out for recording.

Your access depends on the type of account you use to log in. The archives, and live streaming may vary, depending on how archive permission is configured.

To log in to the User Portal:

1. Open a web browser.
2. In the browser address line, enter the system’s portal address, for example, https://System IP
   Note: When an IPV6 address is used, refer to the following format: https://[ipv6]
3. Click Log In at the upper right of the screen.
4. Do one of the following:
   - Enter your user ID and password, then click Log In.
   - To log in as a guest, click Anonymous Access.

- You need to go to Configuration > Portal Settings and clear Disable view permission of user portal for guest user.
- If the Capture Server system is configured with an Active Directory server, users defined on the Active Directory can log in to Capture Server system with their AD account.

To switch to the Admin Portal from the User Portal:

1. In the address line, enter the system’s IP address in this format: https://<system IP address>/.
2. Click Admin Portal, and then enter your user name and password to log in to the system.

RealPresence Capture Server User Portal
You can view live streaming and play back archives from the User Portal.

To view archives and live streams, your device must turn off the pop-up blocker. For example:

- For iPad: From Settings > Safari, make sure the option Block Pop-ups is OFF.
- For Android devices: From Browser > Settings > Advanced, make sure the option Block Pop-ups is OFF.
- For PC Internet Explorer (versions 9, 10, and 11): From Tools > Internet Options > Privacy, make sure the option Turn on Pop-up Blocker is NOT selected.

Manage Archives

From User Portal you can view details of archived files, search archives and play an archived file.

To view archive details:

» Click Archives.

To view the detailed information of the media files, click Details.

To search archives:

1. Click Archives.
2. In the search field at the upper right of the screen, enter the search phrase and then click .

To clear the search result and return to the full view, clear the search phase, and click again.

To play back archives through the User Portal:

1. Log in to the User Portal.
2. Go to Archives.
3 Select the archive you want to play back and click 🎬.

4 A new window opens to play the video.

If the e-mail notification function has been enabled for the VRR that is used to record archives, the system sends you an e-mail notification automatically once all archives have been converted and are ready for web playback. For more information, see Manage Archives.

If your web browser is the Internet Explorer, you may be prompted Display mixed content? When you view a live streaming. Click Yes to proceed. This happens because the User Portal uses secured HTTP (http yet the streaming URL doesn’t. You can change the Internet Explorer’s default security settings from Internet Options > Internet > Custom level > Miscellaneous > Display mixed content > Enable.

View Live Streaming

You can now view live streaming from the User Portal.

To view your live streaming from the User Portal:

1 On a device with compatible web browser, open a supported web browser. See table "User Portal Web Browser Requirement" for the supported web browsers.

2 In the browser address line, enter the system’s portal address, for example, https://System IP.

3 Click Live Streaming from the menu on the left.

4 Click the Play button of the live streaming that you want to play.

The live streaming is opened in a new window.

Call

You can start point-to-point recording or dial our from the Capture Server system through User Portal.

The Call menu is only available after you are logged into the User Portal.

To start point-to-point recording from User Portal

1 In the address line, enter the system’s IP address in this format: https://<system IP address>/portal.

2 Enter the non-admin user name and password to log in to the system.

3 Click Call.

4 Click 2 Sites Recording and enter addresses for two invited participants.

5 Click OK.
Dial out from Capture Server through User Portal:

1. Access Capture Server User Portal by its IP address or host domain name from a compatible browser.
2. Enter the non-admin user name and password to log in to the system.
3. Click Call > Dial out to record.
4. Configure the relevant settings.
5. Click OK.

Dial out to record is also available under Call menu from Admin Portal. The recording starts immediately if Start Recording Immediately is enabled in the selected recording template. For more information, see Configure VRRs.
Appendix A – Console Commands

RealPresence Capture Server supports essential system configuration by using Console. You can access Console via VGA or SSH, some popular applications like Putty supports SSH.

Login Console

The login interface shows all of the software information and you’ll be prompted to enter the login password. Enter the login password and press the Enter key.

The factory default login password is polycom (case sensitive).

If you entered a wrong password, you may be required to re-login to the system.
If you entered the right password, you are brought directly to the command setting interface.

To log in to Console via VGA

1. Connect a monitor and keyboard to the Capture Server system.
2. Enter the user name and password (both are polycom by default)
3. Type Alt+F2 keys to go to the main command menu.

To log in to Console via SSH

1. Open SSH client, enter Host Name and Port (the default SSH port is 22).
2. Enter the user name and password (both are polycom by default)
If you have completed all the above configurations and launched Console successfully, press the **Enter** key. The login interface appears.

**Console Command Descriptions**

You can use the following commands.

**Network Settings**

Select **Network Setting** and type **Enter** to set network configurations (DHCP IP address and static IP address) for LAN 1 or LAN 2.

**To configure Static IP Address for LAN 1 or LAN 2**

1. Choose a network interface, click **OK** or type **Enter**.
2. Select **Static Address Setup**, click **OK** or type **Enter**.
3. Configure network settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the network port</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Gateway address of the network port</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet mask of the network port</td>
</tr>
</tbody>
</table>

4. Click **Save configuration** if you are fine with the settings or **Cancel** to return.

5. The system will show the prompt message **Yes to save the configuration?** Choose **Yes** to proceed or **No** to cancel.

6. At the popup message, click **Yes** if you want the system to restart to apply your changes.
To configure DHCP IP Address for LAN 1 or LAN 2

1. Choose a network interface, click OK and type Enter.
2. Select DHCP Address Setup, click OK and type Enter.
3. Click Set To DHCP.
4. The system will show the prompt message Yes to save the configuration. Choose Yes to proceed or No to cancel.
5. Click Yes if you want the system to restart to apply your changes.

6. Choose DNS Server and type Enter to configure DNS server address for the system to resolve domain names.

Disk Usage

Choose Disk Usage and type Enter to view the disk space usage of RealPresence Capture Server. The total, used, and free disk space are shown.

Reset Console Password

This is to reset the console password, the system will show the prompt message to set new password to access console.

Reset Portal Admin Password

This is to reset the Portal Admin password, the system will show the prompt message to set new password to access the Admin Portal.

Reset Config

This is to reset the following system configurations to the default value:

- System Config
  - Call Settings
  - Signaling Settings
  - Port Settings
  - System time
  - Media Storage Settings
  - Multicast Settings
  - Certificate Management
  - QoS
  - SNMP
  - Active Directory
Appendix A – Console Commands

- Password Settings
- Customization
- Portal Settings

- Admin
  - Log Settings
  - License

- Template
  - Recording Templates
  - Transcoding Templates
  - VRRs
  - Events

- Server
  - IIS
  - WOWZA
  - Windows Media Server
  - AKAMAI

- User
  - User
  - Group

The system will show the following prompt message

![Reset Config]

Click **Yes** to proceed or **No** to cancel.

After resetting the system configuration, the system must be restarted in order for the new settings to take effect.

**Ping**

Choose **Ping** and type **Enter** to check the network connection status.

**Reboot**

Choose **Reboot** and type **Enter** to restart the system. The system will show the prompt message *Do you really want to reboot the machine?* Choose **Yes** to restart the system, or **No** to cancel.
Appendix A – Console Commands

**Shutdown**

Choose **ShutDown** and type **Enter** to power off the system. The system will show the prompt message *Do you really want to shutdown the machine?* Choose **Yes** to restart the system, or **No** to cancel.

**Fallback**

Choose **Fallback** and type **Enter** to restore the system to the time the snapshot was created. Click **Yes** to fall back the system or **No** to cancel.

**Show**

Choose **Show** and type **Enter** to show the general system information including System Version, Interface Information, and IP Address Information.

**Exit**

Choose **Exit** and type **Enter** to exit the command control interface.
Appendix B – Configure 3rd Party Media Servers

You can now stream live meetings and on demand meeting archives to leading 3rd party media servers, such as Wowza, IIS Media Service (Smooth Streaming only) and Windows Media Server. This feature expands the streaming audience capacity of the RealPresence Capture Server system.

Users can watch these streams and on demand meeting archives hosted on external media servers from within the Admin Portal, or from the User Portal.

For more information about Capture Server and Media Manager integration, see the Integration Guide from support.polycom.com.

On the RealPresence Capture Server system, you can live stream recordings and push VoD recordings to the following external media servers:

- IIS Media Server
- Wowza Media Server
- Windows Media Server
- AKAMAI CDN

You can view the live streaming or archives from the User Portal of the RealPresence Capture Server system.

The section shows some useful examples to configure third party external media servers, for latest configuration details, refer to third party external media server documentations.

Configure the Wowza Media Server

You need to configure an Wowza media server and your RealPresence Capture Server to work with the server as well.

1. Install JDK and Wowza. Run
   
   `<Wowza directory>\examples\installall.bat` to create the needed configurations and directories.

Wowza Media Server Configurations and Directories

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Live Streaming</th>
<th>VoD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>live</td>
<td>VoD</td>
</tr>
</tbody>
</table>
Appendix B – Configure 3rd Party Media Servers

To enable Wowza authentication, modify the configuration file as follows:

- For live streaming: Open `<Wowza directory>\conf\live\Application.xml`, set digest as the value for the tag `PublishMethod`. That is, `<PublishMethod>digest</PublishMethod>`.
- For VoD: Open `<Wowza directory>\conf\vod\Application.xml`, Polycom recommends you not to set authentication, make sure `playmethod is none`, `<PlayMethod>none</PlayMethod>`.
- Open `<Wowza directory>\conf\publish.password`, type the your user name and password.

Install and configure a FTP server. The FTP server shares the `<Wowza directory>\content` directory.
You need to grant you at least the Read, Write, and Create Directories authorities.
The following example shows the configuration for a FileZilla FTP server.

Start the Wowza server. When you see the message Wowza media server is started!, the server is started successfully.

To configure the RealPresence Capture Server system for working with the Wowza server:

1. Go to Server > WOWZA.
2. Click Add.
3. Configure the following basic settings

<table>
<thead>
<tr>
<th>Wowza Server Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Specify the name of your Wowza Media Server.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Specify the Wowza server IP address.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Specify the port the Wowza Media Server used to receive live streaming. The value is 1935 by default. Note: Valid port values range from 1-65536. The port number must be the same as set in the corresponding external media server. If a firewall sits between the RealPresence Capture Server system and the external server, make sure that rules are set to allow the two-way communication between the RealPresence Capture Server system and the external server.</td>
</tr>
</tbody>
</table>

4. Specify whether to select Enable Live. If enabled, also configure the following settings:

Enable Live Streaming

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streaming Protocol</td>
<td>Choose between RTSP streaming and RTMP streaming.</td>
</tr>
</tbody>
</table>
Appendix B – Configure 3rd Party Media Servers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Specify the name of the Wowza server application to be used for the live</td>
</tr>
<tr>
<td></td>
<td>streaming. It should be consistent with the Wowza server configuration. In</td>
</tr>
<tr>
<td></td>
<td>this example, application name is live.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specify the user name to access the Wowza media server. This option is</td>
</tr>
<tr>
<td></td>
<td>required when Wowza authentication is enabled. The User Name should</td>
</tr>
<tr>
<td></td>
<td>be consistent with your input in To configure the Wowza server:</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password to access the Wowza media server. This option is</td>
</tr>
<tr>
<td></td>
<td>required when Wowza authentication is enabled. The Password should</td>
</tr>
<tr>
<td></td>
<td>be consistent with your input in To configure the Wowza server:</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the live streaming configurations work.</td>
</tr>
</tbody>
</table>

5 Specify whether to stream video on demand (VoD) from this server.
   - Application Name: the name of the Wowza server application to be used for the VoD.
     It should be consistent with the Wowza server configuration. In this example, application name is VoD.

6 When Enable Vod is selected, configure the following settings to transfer generated recordings to the Wowza server content directory:

Enable VoD

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP Address</td>
<td>Specify the IP address of the Wowza server.</td>
</tr>
<tr>
<td>FTP Port</td>
<td>Specify the port assigned to the Wowza server’s FTP server. The default</td>
</tr>
<tr>
<td></td>
<td>port is 21.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specify your user name to access this FTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify your password to access this FTP server.</td>
</tr>
<tr>
<td>Default Path</td>
<td>Specify the default FTP directory to save your recordings. Use / to</td>
</tr>
<tr>
<td></td>
<td>represent the root directory.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Specify whether to enable SSL encryption for the communication between the</td>
</tr>
<tr>
<td></td>
<td>RealPresence Capture Server system and the FTP server.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the FTP configurations work.</td>
</tr>
</tbody>
</table>

7 Click OK.

- You cannot create two external servers with the same Server type, IP, Port, and Application Name. This is because the RealPresence Capture Server system does not allow publishing two streams to the same publish point to avoid overwriting the first stream by the second one.
- External latency time will be introduced when external media server configured, compared with live streaming from Capture Server, the exact time varies depending on streaming protocol.
To create a VRR for use with an external server:

1. Go to Template > VRRs.
2. Click Add.
3. Configure the following settings:
   - VRR Name:
   - VRR Number
   - Description
   - Recording Template
   - Transcoding Template
   - e-mail Address: select this option and enter one or several e-mail addresses. Separate several addresses with commas (,).
   - The streaming link is contained in the e-mail notification when the streaming is ready for viewing
4. To configure the rest of the settings, refer to the this user’s guide.
5. Click OK.

Configure the IIS Media Server

You need to configure an IIS media server and your RealPresence Capture Server to work with the server as well.

When you configure an IIS media server, you can create two virtual directories, which are used for live streaming and VoDs.

To configure the IIS media server:

1. Launch the IIS manager, then create a virtual directory named as live, with the default port as 80. Specify the physical path for the virtual directory, for example, C:\inetpub\wwwroot\live.
2. Set the authentication methods.
   - Select live.
   - Double click Authentication.
   - To play live streams on an iPad, make sure Anonymous Authentication is selected. To control an IIS publishing point from your RealPresence Capture Server make sure that Windows Authentication is selected.
3. Navigate to C:\inetpub\wwwroot, create two xml files: clientaccesspolicy.xml and crossdomain.xml.

   If you have installed the Polycom RealPresence Media Manager and IIS on the same server, you need to put the correct crossdomain.xml and clientaccesspolicy.xml files to the root directory of the RealPresence Media Manager portal.
   For configuration steps, refer to Capture Server and Media Manager Integration Guide.

   Here is the example text for the clientaccesspolicy.xml and crossdomain.xml files.
Appendix B – Configure 3rd Party Media Servers

- clientaccesspolicy.xml
  ```xml
  <?xml version="1.0" encoding="utf-8" ?>
  <access-policy>
    <cross-domain-access>
      <policy>
        <allow-from http-request-headers="*">
          <domain uri="*" />
        </allow-from>
        <grant-to>
          <resource path="/" include-subpaths="true" />
        </grant-to>
      </policy>
    </cross-domain-access>
  </access-policy>
  ```

- crossdomain.xml
  ```xml
  <?xml version="1.0" encoding="utf-8" ?>
  <access-policy>
    <cross-domain-access>
      <policy>
        <allow-from>
          <domain uri="*" />
        </allow-from>
        <grant-to>
          <resource path="/*" include-subpaths="true" />
        </grant-to>
      </policy>
    </cross-domain-access>
  </access-policy>
  ```

4. Configure a virtual directory for VoDs if you want to play the archives through an IIS Media server.
5. Create a virtual directory named as vod, with the default port as 80. Specify the physical path for the virtual directory, for example, \C:\inetpub\wwwroot\vod.  
6. Install and configure a supported FTP server. The FTP server shares the VoD physical path, for example, \C:\inetpub\wwwroot\vod.  
7. Grant the users at least the Read, Write, and Create Directories authorities.

To configure the RealPresence Capture Server system for work with the IIS server:
1. Go to Server > IIS.
2. Click Add.
3 Configure the following basic settings.

**IIS Media Server Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Specify the name of your IIS Media Server.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Specify the IIS server IP address.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Specify the port that the IIS server used to receive MP4 live streaming. The value is 80 by default. <strong>Note:</strong> Valid port values range from 1 to 65536. The port number must be the same as set in the corresponding external media server. If a firewall sits between the RealPresence Capture Server system and the external server, make sure that rules are set to allow the two-way communication between the RealPresence Capture Server system and the external server.</td>
</tr>
</tbody>
</table>

4 Specify whether to select **Enable Live**. If enabled, also configure the following settings:

**Enable IIS for Live Streaming**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Specify the name of the IIS server application to be used for the live streaming. It should be consistent with the IIS server configuration. In this example, the application name should be live.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specify the user name to access the IIS media server. This field is mandatory for Windows authentication on IIS servers.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password to access the IIS media server. This field is mandatory for Windows authentication on IIS servers.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the live streaming configurations work.</td>
</tr>
</tbody>
</table>

5 Specify whether to stream video on demand (VoD) from this server. If enabled, also configure the following settings:

- Application Name: the application name to access the IIS media server

6 When **Enable VoD** is enabled, configure the following settings to transfer generated recordings to the IIS media server content directory:

**Enable VoD for IIS**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Specify the name of the IIS server application to be used for the live streaming. It should be consistent with the IIS server configuration. In this example, the application name should be live.</td>
</tr>
<tr>
<td>FTP Address</td>
<td>Specify the IP address of the IIS media server.</td>
</tr>
</tbody>
</table>
To configure a template and VRR for use with the IIS server, see To create a VRR for use with an external server:

### Configuring the Windows Media Server

You need to configure an Windows media server and your RealPresence Capture Server to work with the server as well.

To configure the Windows Media Server:

1. Open Windows Media Services on program menu.
2. To enable Windows Media Server authentication, modify the properties as the following:
   - Navigate to **Server > Properties > Authentication**, make sure “WMS Anonymous User Authentication” is enabled.
   - Navigate to **Server > Properties > Authentication**, make sure “WMS Publishing Points ACL Authorization” is enabled, and the Everyone user has full permission.
   - For live publish point, RSS can create the live publish points, so don’t need to create it manually at Windows Media server.
   - For vod publish point, Create a On-demand publish point, input publish point name, location of content, for example, c:\WMpub\WMarchive.
3. Install and configure an FTP server. The FTP server shares the c:\WMpub\WMarchive directory. You need to grant the user at least the **Read, Write, and Create Directories** authorities.

To configure the Capture Server system for work with the Windows Media server:

1. Go to **Server > Windows Media Server**.
2. On the **ACTION** panel, click **Add**.

<table>
<thead>
<tr>
<th>FTP Port</th>
<th>Specify the port assigned to the IIS media server's FTP server. The default port is 21.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Specify your user name to access this FTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify your password to access this FTP server.</td>
</tr>
<tr>
<td>Default Path</td>
<td>Specify the default FTP directory to save your recordings. Use / to represent the root directory.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>Specify whether to enable SSL encryption for the communication between the RealPresence Capture Server system and the FTP server.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the FTP configurations work.</td>
</tr>
</tbody>
</table>
Appendix B – Configure 3rd Party Media Servers

3 Configure the following basic settings.

**External Media Servers Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Specify the name of the external server.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Specify the IP or DNS of the external server you selected.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>The default value is 80.</td>
</tr>
<tr>
<td>RTSP Port</td>
<td>The default value is 554.</td>
</tr>
</tbody>
</table>

4 Specify whether to select **Enable Live**. If enabled, also configure the following settings:

**Enable Live Streaming**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Specify the user name to access the external media server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password to access the external media server.</td>
</tr>
<tr>
<td>Test</td>
<td>Test whether the live streaming configurations work.</td>
</tr>
</tbody>
</table>

5 Specify whether to stream video on demand (VoD) from this server. If enabled, specify the application name. The application name is the name of the media server’s application to be used for VoD.

Contact the administrator of the external media server for the naming rule of the application name.

6 When **Enable VoD** is selected, configure the following settings to transfer generated recordings to the pre-installed FTP server of the external server:

**Enable VoD**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publishing Point</td>
<td>Specify a publishing point for Windows Media Server.</td>
</tr>
<tr>
<td>FTP Address</td>
<td>Specify the IP or DNS of the external server’s FTP server.</td>
</tr>
<tr>
<td>FTP Port</td>
<td>Specify the port assigned to the external server’s FTP server. The default port is 21.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specify your user name to access this FTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify your password to access this FTP server.</td>
</tr>
<tr>
<td>Default Path</td>
<td>Specify the default FTP directory to save your recordings. Use / to represent the root directory.</td>
</tr>
</tbody>
</table>
### Parameter | Description
--- | ---
Enable SSL | Specify whether to enable SSL encryption for the communication between the RealPresence Capture Server system and the FTP server.
Test | Test whether the FTP configurations work.

7. Click **OK**.
Appendix C – Configure the Server Working with VCS

This chapter demonstrates how to configure RealPresence Capture Server working with Cisco TelePresence® Video Communication Server (Cisco VCS). The configurations are different between H.323 and SIP.

- Configure VCS for H.323 Calling
- Configure VCS for SIP Calling

Configure VCS for H.323 Calling

For H.323, after you register RealPresence Capture Server to the Cisco VCS, Cisco VCS works as a gatekeeper. you can configure the Cisco VCS and then call a VRR created on RealPresence Capture Server to start a recording.

To configure VCS calling:

1. Create authentication accounts in VCS, such as ff1/1234, ff2/1234….ff6/1234.
2. Register RealPresence Capture Server to VCS. See To register the system to a gatekeeper to make H.323 calls: for detailed steps.
3. Go to Configuration > Signaling Settings and set Gatekeeper type as Cisco VCS.
4. Register an endpoint to the VCS. For example, register Polycom Group Series 500 to the VCS.

Now you can dial from the Group Series 500 and the format of the address is E.164+VRR Number. After the call is set up successfully, you can check the RealPresence Capture Server Admin Portal.

Configure VCS for SIP Calling

If your network supports SIP, you can use SIP to connect to conference calls. Cisco VCS works as a SIP server.

To configure VCS for SIP calling:

1. Register RealPresence Capture Server to VCS via SIP. See To configure the SIP settings: for detailed steps.
2. Register an endpoint to the VCS via SIP. For example, register HDX 4000 to the VCS.
3. Configure the VCS to enable SIP calling.
   a. Log in to the Cisco VCS as an administrator.
   b. Go to VCS Configuration > New zone to create a new zone.
Configure the zone for your RealPresence Capture Server. Refer to the following table.

**VCS Zone Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>capture_server_zone</td>
</tr>
<tr>
<td>Type</td>
<td>Neighbor</td>
</tr>
<tr>
<td>Hop count</td>
<td>15</td>
</tr>
<tr>
<td>H.323 Mode</td>
<td>On</td>
</tr>
<tr>
<td>H.323 Port</td>
<td>1719</td>
</tr>
<tr>
<td>SIP Mode</td>
<td>On</td>
</tr>
<tr>
<td>SIP Port</td>
<td>5060</td>
</tr>
<tr>
<td>SIP Transport</td>
<td>TCP</td>
</tr>
<tr>
<td>Accept proxied registration</td>
<td>Allow</td>
</tr>
<tr>
<td>Authentication policy</td>
<td>Do not check credentials</td>
</tr>
<tr>
<td>SIP authentication trust mode</td>
<td>Off</td>
</tr>
<tr>
<td>Peer 1 address</td>
<td>Your RealPresence Capture Server IP address.</td>
</tr>
<tr>
<td>Zone profile</td>
<td>Custom</td>
</tr>
</tbody>
</table>
d Create a search rule to route to the zone you created.
The following example assumes that you have the default tandberg recommended rules in place.

**Set search rule parameters**

![Image of search rule configuration settings]

Now, you can start a recording by calling a VRR number from any endpoint registered to this Cisco VCS. For example, if the VRR number is 12345, you can dial 13913912345 directly to start a recording. 139139 is the prefix name (pattern string set in above picture).