User Guide

Version 1.6.1 | Release Date (August 2014) |3725-69804-002/A

Polycom® RealPresence® Capture Server - Virtual Edition User Guide

Copyright© 2014, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

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

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

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

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you.

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

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

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

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

Contents

System Overview

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

Feature	Description	Maximum Record Port 6 port license
Signaling Connection (H323/SIP)	Specify the maximum number of devices connected to RealPresence Capture Server simultaneously. Connection type: live streaming recording, recording only, and playback.	6
Conference Recording	Specify the maximum number of conferences that can be recorded simultaneously. Connection type: recording only.	6
Single-point Conference Live Streaming	Specify the maximum number of single-point conferences that can be live streamed simultaneously. **Note:** The conference being live streamed can also be recorded.	3 (720p) 6 (4CIF)

Live Streaming Resources Usage

The combination of frame rate, resolution, number of rates used and video layout affects the number of resources required on the RealPresence Capture Server to support live streaming. For information about setting the rates and the video layout, see Live Streaming .

The following live streaming recording properties determine the required system resources. The video of people and content is in a single window.

- Single System Resource Required
  - Recording resolution (people): CIF, 4CIF, and 720p 30 fps
  - Recording resolution (Content): XGA 7.5fps, and 720p 30 fps
  - Stream rates: only use primary rate.
- Two System Resource Required
  - Recording resolution (people): CIF, 4CIF, and 720p 30 fps
  - Recording resolution (Content): XGA 7.5fps and 720p 30 fps
  - Stream rates: use primary and secondary rate.

Consider the 6/3 ports license that supports up to three live streaming, for example. If there is an ongoing live streaming sending video at 720p 30 fps using primary rate (1024 Kbps) and secondary rate (832 Kbps),

this uses two resources on the system. One resource is free, which allows for running one live stream at CIF/4CIF/720p 30 fps, using only primary rate concurrently.

RealPresence Capture Server Stand-alone Unicast Live Streaming and VoD

The maximum number of web connections supported by the RealPresence Capture Server system to view playback or live streaming simultaneously is as follows:

- 768K~1728K: 250
- 1920K~4096K: 125

RealPresence Capture Server can support up to 500 total web viewers of any combination of 512k streams (VoDs and live stream).

RealPresence Capture Server and External Stream Servers

The capacity depends on RealPresence Capture Server system's Viewer Portal login capacity and external stream server capacity. For external stream server capacity, see the official website of external stream servers.

Multi-user Login Capacity

The maximum number of admin UI login and Viewer Portal login (including anonymous login) is as follows:

- Admin UI Login: 200
- Viewer Portal Login: 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.

User Interfaces

RealPresence Capture Server provides four interfaces that are used for specific purposes:

Web-based Admin Portal

This section introduces how to access the web-based Admin UI and its fundamental layout. You can access the Admin UI via a compatible web browser, the Admin UI is used to configure the system, set up recording parameters, monitor system use and health, dial out to endpoints to record meetings, disconnect calls in progress, 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 UI at the same time.

The following sections present an overview of RealPresence Capture Server to help you get started:

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 and conference platforms 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 720p 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 is best when integrated with the Polycom RealPresence Media Manager version 6.6 for enhanced content management, auto-publishing, and streaming scalability.

Accessed via a compatible web browser, the Admin Portal is used to configure the system, set up recording parameters, monitor system use and health, dial out to endpoints to record meetings, disconnect calls in progress, 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.

Polycom now offers a virtual edition of the RealPresence Capture Server system, this edition is packaged as an Open Virtualization Archive (OVA) file. The OVA file contains the RealPresence Capture Server application and information about its virtual machine environment. It can be installed as a virtual instance on a host machine running VMware vSphere.

User Permissions through Admin UI

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

User Permissions

Content	Auditor	Administrator
Accessible information	System logs	All pages
Operation permissions	View and download system logs.	View, edit, and delete

To log in to the Admin UI:

1. In the address line, enter the system's IP address in this format: http://<system IP address>/admin.

   Whenever you access the Admin UI without a supported security certificate installed, you will see a certificate error. To avoid this error, you need to install a supported certificate. See Install the Certificate in the System for details.

   When an IPV6 address is used, a port number must be added. For example:
   `http://[ipv6]/admin`
   `http://[ipv6]/admin`

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

   When using Internet Explorer to configure the RealPresence Capture Server system, always enter the address of the system in this format: http://<system IP address>/admin> or http://captureserver01.acme.com, for example, http://10.11.12.13/admin.

   Using the HTTP 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 HTTP protocol limits the ability of anyone monitoring traffic on the network to discover these credentials.

Web-based Viewer Portal

Accessed via compatible device/web browser (PC/MAC, iOS and Android), the Viewer Portal UI is used to find, navigate, search, play archives and live streams.

Search and Refresh Lists

You can search items listed on the Admin UI, for example, the VRR list and user list.

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.

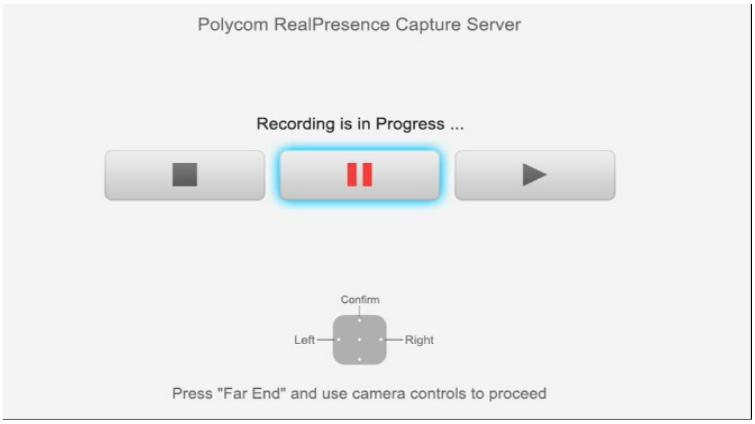
TV user interface (also called the “TVUI”)

Accessed via standards-based video conferencing endpoints, this interface can be used to record meetings.

Understand the Main Menu

In addition to the Admin UI, the RealPresence Capture Server system also provides a TV user interface for you to perform the most commonly used operations using the remote control. 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

Scenario	FECC	Description	DTMF	Description
When in the menu display state		Pause the recording.	*1	Pauses the recording.
		Confirm the selection.	*2	Starts or resumes a paused recording.
		Select leftward (cyclic).	*3	Stops the recording.
		Select rightward (cyclic).	*5	Plays back the recording.
When in the video playing state	-	-	*1	Pauses the current video.
	-	-	*2	Starts or resumes a paused video.
	-	-	*3	Stops playback of the current video and returns to the main menu.
	-	-	*4	Reverses the current video.
			*6	Fast forwards the current video.

Console

Accessed via vSphere client console or SSH, console is used to view/change IP settings and reboot the system.

Hardware Installation

Hardware Requirements

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

Hardware RequirementS

Component	Description
Virtual Cores	Each instance must have more than 8 virtual cores. Also see Resource and License Management .
CPU	The recommended CPUs are: 2.67GHz (Intel® Xeon® CPU x5650@ 2.67GHz or better) CPU 2.90GHz (Intel Xeon CPU E5-2690 @ 2.90GHz or better) CPU
Minimal RAM	16 GB
Minimal Accessible Storage	120 GB
NFS Storage	Refer to the media storage disk space warning threshold set under **Configuration > Media Storage Setting,** this value should not be less than this threshold value.

Software Installation

Software Requirements

RealPresence Capture Server - Virtual Edition is supported on VMware vSphere 5.1/5.5. Before you install and configure the RealPresence Capture Server system, you need the following:

- VMware vSphere 5.1/5.5 client installed where you can access the ESXi host
- Login credentials and IP addresses of one or more VMware vShpere hosts on which you will deploy your RealPresence Capture Server OVA
- A web browser where you access the Viewer Portal. See table "Viewer Portal Web Browser Requirement" for the supported versions

Resource and License Management

A RealPresence Capture Server license is required to enable you use this product with the full capabilities. The RealPresence Capture Server capability is determined by the license and the virtual cores of each VMware RealPresence Capture Server instance. See the following table for licenses and their corresponding CPU cores requirements.

Resource and License Management

License	Virtual CPU Cores
6 Calls Record 3 Calls (of the 6 total calls) stream live	CPU cores are between 8 and 16.

Web Browser and OS Requirements

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

Viewer Portal Web Browser Requirement

Set up RealPresence Capture Server in a Virtual

Operating System	Browser Name	Version	MP4 (Live stream &VoD)
PC (Windows 7, and Windows 8)	Internet Explorer	9, 10, 11	Yes
	Firefox	26, 27	Yes
	Chrome	32, 33	Yes
MAC OS-X (Intel-based Leopard, Snow, and Lion)	Safari	7.0.1	Yes
	Firefox	26, 27	Yes
	Chrome	32, 33	Yes
iOS (iPad 2/air/mini, iPhone 4S/5)	Safari	6.1.3, 7.0.3	Yes
Android Tablet (Samsung GT-P5210 and GT-N5100)	Android browser	4.1.2, 4.3	Yes
Android Phone (Samsung Galaxy S4 and Galaxy Note3)	Android browser	4.1.2, 4.3	Yes

Environment

The following steps assume you are familiar with deploying applications into a VMware environment.

For more information about deploying applications into a VMware environment, see the VMware documentation.

To set up RealPresence Capture Server in a virtual environment:

1. Obtain the RealPresence Capture Server OVA package.

2 Deploy the OVA file into the VMware vShpere hosts that you have set up.

If the VMware vSphere host is very busy or it does not match the RealPresence Capture Server hardware requirements, the deployment may fail. See table "Hardware RequirementS" for more about hardware requirements.

3 From the vSphere client, select the virtual instance you installed and power it on.

4 Click the **Summary** tab and note the temporary IP address of RealPresence Capture Server system assigned by DHCP.

Configure NFS

Once the NFS share is configured, clients use the `mount` command to mount the share. Once mounted, the share appears as just another directory on the client system. Some Linux distributions require the installation of additional software to mount an NFS share. On Windows systems, enable Services for NFS in the Ultimate or Enterprise editions or install an NFS client application.

To export a shared storage location via NFS on a typical Linux system, CentOS used in below example

1 Make sure the NFS service has been installed and is running.

Examples:

```
[root@centos-nfs ~]# service nfs status
rpc.svcgssd is stopped
rpc.mountd (pid 20129) is running...
nfsd (pid 20194 20193 20192 20191 20190 20189 20188 20187) is running...
rpc.rquotad (pid 20125) is running...
```

2 Edit the NFS configuration file /etc/exports to set the file system paths for export.

Examples:

```
[root@centos-nfs ~]# cat /etc/exports
/home/nfs *(rw,no_root_squash)
/home/nfs_zip_1 192.168.9.78(rw,no_root_squash)
```

3 Restart the NFS service.

Examples:

```
[root@centos-nfs ~]# service nfs restart
Shutting down NFS daemon:                                  [  OK  ]
Shutting down NFS mountd:                                  [  OK  ]
Shutting down NFS quotas:                                  [  OK  ]
Shutting down NFS services:                                [  OK  ]
Starting NFS services:                                     [  OK  ]
Starting NFS quotas:                                       [  OK  ]
Starting NFS mountd:                                       [  OK  ]
Stopping RPC idmapd:                                       [  OK  ]
Starting RPC idmapd:                                       [  OK  ]
Starting NFS daemon:                                       [  OK  ]
```

4 Go to **Configuration > Media Storage Settings** and configure the settings.

Product Activation

Obtain the Product Activation Key from Polycom

A new installation of RealPresence Capture Server version 1.6 Virtual Edition comes with a 90-day trial license. 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 v1.6.

To obtain the product activation key:

1 Go to **Admin > Product Activation** to locate the serial number. 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 When you are logged in, click **SITE & Single Activation/Upgrade**.

7 Enter the **Serial Number** you recorded and click **Next**.

8 When prompted, acknowledge and accept the **Export Restrictions agreement**.

9 Follow the page prompts step by step to generate the Key Code required for system activation.

If you are required to enter the **License Number and Serial Number** of the system, you can find them from the document provided with RealPresence Capture Server.

10 Note the activation key (Key Code) on the page and click **Upgrade**.

After you get your activation key, you need to use it to activate your system.

Activate Product and Check the Activation Status

To view the system activation status:

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

Parameter	Description
License Type	Permanent license or 90-day trial version
Software Version	Current version of the software running on the system
Serial Number	Product serial number
Activation Status	Whether the system is activated;  indicates activated system, and  indicates it is not activated
Max Recording Ports	Maximum number of recording ports supported by the system
Max Live Streaming Ports	Maximum number of live streaming ports supported by the system
Max Streaming Sessions	Maximum number of video-on-demand and live streaming supported by the system. Base: 250. Note: After purchasing and activating the license, the streaming sessions capacity will be increased from 250 to 500.
Media Encryption	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. When the encryption function is activated,  displays; otherwise,  displays.
HD Live Streaming	Whether the high resolution live streaming function of the system is activated. This is a charged function. You can use it only after purchasing the license and activating it. Once this function is activated, the system can live stream 720p resolution videos.
Streaming without recording (no archive)	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.
Basic Timecode Watermark	Whether the basic timecode watermark capability for transcoded mp4 on-demand files is activated. This is activated by default, mp4 on-demand archives can be output with basic timecode watermarking.

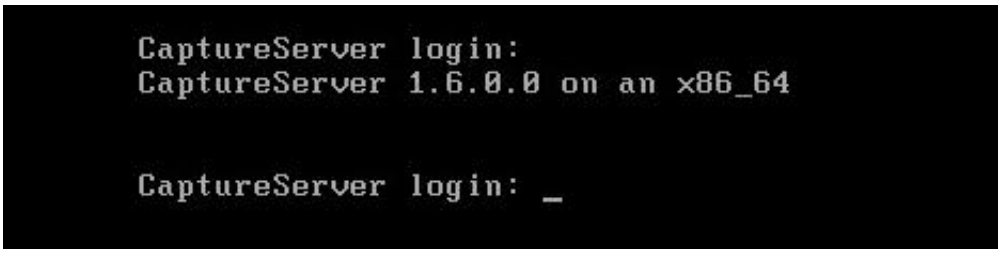
System Initialization

Configure IP Settings through Console

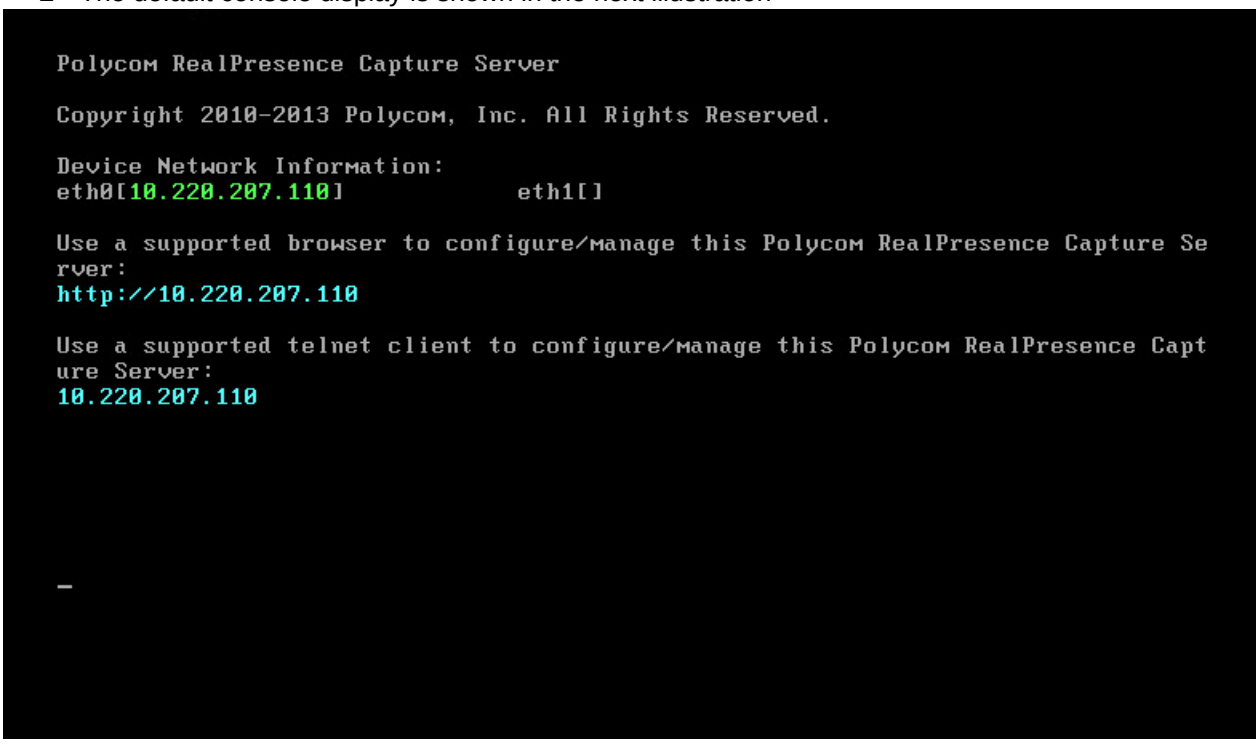
By default, when a new RealPresence Capture Server is started, it obtains an IP address from the DHCP server automatically. Follow the steps below to check the IP address assigned by DHCP server.

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

1 Open the console of your RealPresence Capture Server.



2 The default console display is shown in the next illustration



3 The IP address displayed on console is shown in the above illustration, for example: **http://10.220.207.110**

Two ways are available for setting the system IP:

- If you do not have a DHCP server in your network, you can assign the system a static IP from the RealPresence Capture Server's console.
- If you have a DHCP server in your network, you can modify the RealPresence Capture Server IP address in the Admin UI. See To change the system's initial IP settings from the Admin Portal:

4 Type **Alt+F2** keys to go to the login screen.

5 Enter the user name and password (both are **polycom** by default).

6 After logging into the system, you may enter *?* or help after the prompt # to show the command prompt information.

7 Set RealPresence Capture Server a static IP for LAN interface using the commands shown in the following table. For normal usage, only LAN1 IP address setting is required.

Command	Description
`set {lan1 | lan2} ip static {ip} netmask {mask } gw {gateway}`	Set the IP address for LAN1. For example, `set lan1 ip static 192.168.1.254 netmask 255.255.255.0 gw 192.168.1.1`

8 After you set the IP, restart the system to apply the changes.

Configure IP Settings through Admin UI

Configure the IP Parameters

TheRealPresence 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, 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

Parameter	Description
Enable Network Separation	Select this check box to route the management traffic and signaling traffic through LAN 1 and LAN 2 interfaces separately. This offers higher security for the signaling data.
Obtain an IP Address Automatically (DHCP)	If you select this radio button, RealPresence Capture Server obtains an IPv4 address automatically via DHCP. **Note:** Obtaining an IP address automatically is not recommended. For best results, assign a static IP to RealPresence Capture Server.
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.
Enable ICMP V6 DAD	Specify whether to enable Duplicate Address Detection (DAD) to ensure the IPv6 address set to the system is unique in the local network.
Enable ICMP Echo	Specify whether to allow the system to respond to an ICMP (Internet Control Message Protocol) echo request (Ping) sent from other devices in the network. In some high-security environments, you may need to disable this option to protect the system from Ping attacks.
MTU	Specify the Maximum Transmission Unit (MTU) size.

LAN Speed	Specify the speed or duplex modes for the LAN port. Select **Auto** to let the system set the speed automatically. **Note:** When setting the LAN port speed, contact your network administrator to ensure that the switch link rate matches the system port speed.
NAT Public (WAN) Address	Set the external IP address in Network Address Translation (NAT) environment. NAT environments use private internal IP addresses for devices within the network, while using one external IP address to allow devices inside the LAN to communicate with other devices outside the LAN.

2 Configure the following general settings:

General System Network Parameters

Parameter	Description
Host Name	Specify the host name of the system.
Domain	Specify the domain name of the system.

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

Set Route Parameters

Parameter	Description
Destination	Specify the IP address of the destination network.
Gateway	Specify the IP address of the gateway to access the destination network.
Subnet Mask	Specify the subnet mask for the destination network.

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

To activate the system and change the system's initial IP settings from the Admin UI:

1 Enter the following website address in the address bar of the web browser: http://10.220.207.110/admin.

2 (Optional) Click **Select language** and select a language for the Admin UI.

3 Enter the default administrator's user name (*admin*) and password (*Polycom123*), and then click **Log In**.

4 Change your password and then click **OK**.

5 Go to **Product Activation** page, enter the activation key and click **Update**.

When you copy and paste activation keys, it is best to paste into Notepad first to remove any formatting and ensure no trailing spaces are left in the activation. Copy only the key, paste into the Activation field.

6 Select **Reboot Later** to proceed with setting the IP address.

7 Go to **Configuration > IP Settings** and configure the network settings.

- Select **Using the following IP** radio button if you want to set a static IP to RealPresence Capture Server. Enter the IP address and subnet mask.
- Specify the general system network settings:
  - 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.

Use the default values for other fields.

System Administration

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

Parameter	Description
Far End Number	The far end number used by the connection.
Start Time	When the calls started.
Signaling Type	H.323 or SIP.
Dial In/Out	Whether the connection is incoming or outgoing.
VRR Number	The VRR number used by the connection.
Live Streaming	Whether the connection is performing live streaming.
Detail	Additional information like Signaling Type, Dial In/Out, Far End Number, VRR Number, VRR Name, Audio Type, Video Type, Status, Live Streaming, and Encryption.

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**.

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.
- The activation statuses of the charged options.

System Alerts

Shows the system alert information.

Signaling Server Status

Displays gatekeeper registration status and SIP server registration status. When the 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**
  - **CPU Usage**
  - **Memory Usage**
  - **System Disk Usage**
- **Extension**

External Server Status

The system can be integrated with external servers, such as IIS and WOWZA. External server status indicates the connection status between the system and the server. You can check the status for IIS, WOWZA and NFS server respectively.

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

Adding an User

Parameter	Description
User ID	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 "_" symbol characters. Once created, user ID cannot be modified.
Full Name	Specify the user's full name.
Password	Specify the login password.
Confirm Password	Specify the confirmed password which must be identical to the login password.
Role	User roles: **Administrator**, **Auditor** or **User**. Different roles determine the user operation permissions after logging in to pages.
Description	Specify additional related information.

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.

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:

» Go to **User > 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, double-click it.

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 here. 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

Parameter	Description
Allow recording even when no resources are available to create live stream(s).	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.
Key Frame interval	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 **Fast forward** 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.
Indication Tone	Played to indicate that recording is ongoing, typically it is a very short beep with intervals between beeps, measured in second.
Media Encryption	If the Capture Server is licensed for call encryption, this option specifies how AES (Advanced Encryption Standard) encryption is enabled for H.323 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 for H.323 and SIP connections when the peer device enables the AES option, and vice versa. • **Off:** Disable the AES encryption for H.323 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.

Configure Signalling 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.

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: http://<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

Parameter	Description
Gatekeeper type	The default gatekeeper is Polycom.
Primary Gatekeeper	Indicates whether the system is registered to the primary gatekeeper.
Gatekeeper Address	Specify the IP address for the gatekeeper.
Gatekeeper Port	Specify the port number for the gatekeeper, the default value is 1719.
Register User Information for Gatekeeper	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.
Gatekeeper User	Specify the user name for registration with the Polycom Gatekeeper server.
Gatekeeper Password	Specify the password for registration with the Polycom Gatekeeper server.
Alternate Gatekeeper	Indicates whether the system is registered to the alternate gatekeeper. **Note**: The alternate gatekeeper is used only when the primary gatekeeper is not available.
System Prefix / E.164	Specify the E.164 number for the system.
System H.323 Alias	Specify the H.323 alias for the system.
Remote Display Name	Specify the name to be displayed to the far end. Note: If you set the remote display name with dual-bytes characters like Chinese, you will not see the characters on the far end endpoints in a H.323 call between endpoints and the Capture Server system.

SIP

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

To configure the SIP settings:

1. Go to **Configuration > Signaling Settings > SIP**.

2 Configure the following settings:

SIP Parameters

Parameter	Description
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 the IP address, connection port, and domain name of the SIP server for registration service.
Register User Information	Specify the user name and password that authenticates the system to the SIP Server.
Outbound Proxy Server	For communication with the SIP server when the system is configured on the internal network, an outbound proxy server is required to implement traversal of the firewall or NAT. In this case, you need to set the IP address and port number for the outbound proxy server.

3 Click **OK**.

(Optional) Configure the Gatekeeper Settings

If a gatekeeper is configured on your network, register RealPresence Capture Server to the gatekeeper 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: http://<system IP address>/admin.

2 Go to **Configuration > Signaling Settings > H.323**.

3 Select **Register To Gatekeeper**.

4 Configure the settings list in the following table. After you finish the configuration, click **OK**.

H.323 Gatekeeper Parameters

Parameter	Description
Gatekeeper type	Choose between **Polycom** and **Cisco VCS**.
Primary Gatekeeper	Indicates whether the system is registered to the primary gatekeeper.

Gatekeeper Address	Specify the IP address for the gatekeeper.
Gatekeeper Port	Specify the port number for the gatekeeper, the default value is 1719.
Register User Information for Gatekeeper	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.
Gatekeeper User	Specify the user name for registration with the Polycom Gatekeeper Server.
Gatekeeper Password	Specify the password for registration with the Polycom Gatekeeper server.
Alternate Gatekeeper	Indicates whether the system is registered to the alternate gatekeeper. Note: The alternate gatekeeper is used only when the primary gatekeeper is not available.
System Prefix / E.164	Specify the E.164 number for the system.
System H.323 Alias	Specify the H.323 alias for the system.

Configure Port Settings

Port Settings allow specific ports in the firewall 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:

Port Parameters

Parameter	Description
TCP Ports	Specify the TCP port range. You can set the starting port number, and the ending port number is calculated automatically.
UDP Ports	Specify the UDP port range. You can set the starting port number, and the ending port number is calculated automatically.
Streaming Port	Specify the streaming port range.

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

Set the System Time

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

To set the system time:

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

System Time Parameters

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

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

Configure Media Storage Settings

By default, RealPresence Capture Server stores the files on a network file system if you enable it.**To save your files on a network file system:**

1. Click **Configuration > Media Storage Settings**.
2. Configure the following settings for the network file system.

Media Storage Setting

Parameter	Description
NFS Server Name	Optional. Enter a name for the NFS server.
NFS Server Address	Enter an address of the NFS server.
NFS Storage Folder	Specify the folder path to the NFS storage. Note: Make sure the NFS server is set up beforehand.
Test	Test whether the NFS server is reachable.

Synchronize archives when storage setting changed	When this option is checked, the archives on the storage will be synced up with the archive record in the system database, and could be viewed from portal (viewer or admin). The sync-up action takes effect after the system restarts.
Send warning e-mail to Admin when remaining NFS free space reaches: (GB)	Set a NFS storage space threshold. You can set a value in the range of 10-50GB. After the system reaches the threshold, RealPresence Capture Server will send notifications to specified receivers.

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

If Network storage is disabled or error, RealPresence Capture Server cannot dial in and dial out.

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)
- 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 UI

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

Type	Description
.pem	Privacy Enhanced Mail, base64 encoded DER certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".
.cer, .crt, .der	Usually in binary DER form, but Base64-encoded certificates are also common (refer to .pem).
.p7b, .p7c	PKCS#7 SignedData structure with certificates or CRLs and without data.
.p12	PKCS#12, may contain public certificates and password-protected private keys.
.pfx	PFX, predecessor of PKCS#12. This type usually contains data in PKCS#12 format, for example, with PFX files generated in IIS.

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-----. If it is a file, it can be either PEM or DER encoded.

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

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

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 using e-mail or 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

Parameter	Description
Certificate Info	States the purpose and alias of the certificate.
Issue To	States the entity to which the certificate was issued and the certificate serial number.
Issue By	States the issuer.
Validity	States the issue and expiration dates.
Fingerprints	States SHA1 and MD5 fingerprints (checksums) for confirming certificate.

When a certificate is about to expire, you are notified ten days prior to the expiration date.

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

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

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

Parameter	Description
Enable QoS for Signaling and Media	Enable configuration of the QoS settings. if not selected, the system uses the default QoS settings.
Type	**DiffServ** and **Precedence** are two methods for encoding packet priority. The priority set here for audio and video packets should match the priority set in the network routers. • **Differv**: Select when the network router uses **Differv** for priority encoding. If this option is selected, enter values in the **Audio** and **Video** fields. The value range is 0-63. **Note:** If you select **DiffServ** but your router does not support this standard, IP packets queue on the same communication links with data packets. This non-prioritized queueing greatly increases the latency and jitters in their delivery and can negatively impact performance. • **Precedence**: Select this option when the network router uses **Precedence** for priority encoding, or when you are not sure which method is used by the router. **Precedence** should be matched with **None** in the **ToS** field. The value range is 0-5. If this option is selected, enter values in the **Audio** and **Video** fields. The value range is 0-5. **Note: Precedence** is the default mode as it is capable of providing priority services to all types of routers and is currently the most common mechanism.
Audio / Video	Specify the priority for audio and video IP packets. The recommended priority is 4 for audio and video to ensure that the packet delay for both is the same, that audio and video packets are synchronized, and to ensure lip and audio synchronization (lip sync).
Control	Specify the priority for controlling packets.
ToS	Select the ToS (Type of Service) that defines optimization tagging for routing the conference audio and video packets. • **Delay:** The recommended default for video conferencing: prioritized audio and video packets tagged with this definition are delivered with minimal delay. • **None:** No optimization definition is applied. This is a compatibility mode in which routing is based on **Precedence** priority settings only. Select **None** if you do not know which standard your router supports.

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

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

Parameter	Description
Download MIB Files	Download MIB file to your computer.
Agent Name	Specify the name of this RealPresence Capture Server agent.
Contact Country	Specify the contact country for this RealPresence Capture Server.
Contact Person	Specify a contact person for this RealPresence Capture Server.
SNMP Agent Version	Specify the SNMP Agent version.

4. Configure the following security settings:

Security Settings

Parameter	Description
Accepted Host Community Name	Specify the community name that the host belongs to.
User Name	Specify the user name that will be used to log in over the **Authentication Protocol**.
Authentication Protocol	Specify the type of encryption to use when connecting with this user: • **MD5**: Message Digest 5 • **SHA**: Secure Hash Algorithm
Authentication Password	Specify the password that will be used to log in over the **Authentication Protocol**. **Note**: A valid password contains 8-64 characters, and not include these characters: &,',",<,>,%,|,+,=
Privacy Protocol	Specify the privacy protocol that you want to use: • **DES**: Data Encryption Standard • **AES**: Advanced Encryption Standard
Privacy Password	Specify the password that will be used to log in over the privacy protocol. **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 > Download 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.**

Redirect Visitors to the Media Manager Home Page

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.

To enter a redirect URL:

1. Go to **Configuration > Portal Settings.**
2. Enter a URL and click **Test**.
3. Click **OK.**

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.

Security Policy Parameters

Parameter	Description

Password Management	Password Expired Warning Period	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
	Maximum Password Age	Specify the maximum number of days that can pass before the password must be changed. Default: 90
	Minimum Password Age	Specify the minimum number of days that must pass before the password can be changed. Default: 0
	Reuse Number of Password	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
Password Complexity	Allow to contain or reverse User ID	Specify whether to allow a valid password to contain the same characters, in the same order or reversed, as the user name.
	Minimum Password Length	Specify the minimum number of characters required for a valid password. Default: 1
	Minimum Password Changed Characters	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
	Maximum Consecutive Repeated Characters	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
	Minimum Upper Case	Specify the minimum number of uppercase characters required for a valid password. Default: 0
	Minimum Lower Case	Specify the minimum number of lowercase characters required for a valid password. Default: 0
	Minimum Numeric Characters	Specify the minimum number of numbers required for a valid password. Default: 0
	Minimum Special Characters	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

The value 0 indicates no limitation to this option.

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**.

Setup E-mail

You can set an e-mail address for your RealPresence Capture Server system. This is filled to “From” address in the email 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 Emaill Notifications:** When enabled, you receive e-mail notification when live streaming starts or transcoding is done.

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 viewer portal to the Media Manager (or 3rd party portal)’s user portal.

To enter a redirect URL:

1. Go to **Configuration > Portal Settings.**
2. Enter a URL and click **Test**.
3. Click **OK.**

Record and Playback

Configure Templates

A template is used to define a set of basic recording link parameters, such as the bandwidth for recording and live streaming, video quality, and whether to live stream. 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

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:

Recording Template

Parameter	Description
Template Name	Specify a unique name to identify this template.
Enable Live Streaming	Select this check box to enable live streaming for the system.
Enable PIN	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**.
Audio Only	Select this check box to define the recording for the call with this template has only audio capability, no matter the call rate negotiated.
Max Call Rate	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.

Max Resolution	Specify the maximum resolution that can be used to connect to the RealPresence Capture Server system for recording and live streaming.
Enable LPR	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.
Indication Tone	Played to indicate that recording is ongoing, typically it is a very short beep with intervals between beeps, measured in second.
Media Encryption Type	If the Capture Server is licensed for call encryption, this option specifies how AES (Advanced Encryption Standard) encryption is enabled for H.323 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 for H.323 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.
Start Recording Immediately	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 UI or the TV UI.
Archive Name Prefix	Specify the prefix of the output media archive name.
Enable H.264 High Profile for Live Streaming	Select this check box to enable the use of H.264 High Profile in Video Switching conferences.
Primary Streaming Rate (Kbps)	The default value is 1024 kbps.
Secondary Streaming Rate (Kbps)	The default value is **Off**.

Layout	Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts: • **Single window with small content (People 75%; Content 25%):** Displays dual stream in one window of which 75% is people video and 25% content video. • **Single window with medium content in right (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video at the right side. • **Single window with medium content in left (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video at the left side. • **Single window with large content (People 25%; Content 75%):** Displays dual stream in one window of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent.
Primary Streaming Rate (Kbps)	The default value is **Off**.
Secondary Streaming Rate (Kbps)	The default value is **Off**.
Layout	Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts: • **Single window with small content (People 75%; Content 25%):** Displays dual stream in one window of which 75% is people video and 25% content video. • **Single window with medium content in right (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video. • **Single window with medium content in left (People 50%; Content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video. • **Single window with large content (People 25%; Content 75%):** Displays dual stream in one window of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent. • **Dual window for content (when inactive content, it is black):** 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.

4 Click **OK**.

You can click **Save As** to rename the template.

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**.

Configure Transcoding Template

To view a transcoding template:

» Go to **Template > Transcoding Templates**.

To define a transcoding template:

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

Transcoding Template

Parameter	Description
Template Name	Specify a unique name to identify this template.
Media Type	Specify the output media file format.
Bit Rate	Specify the output media file bitrate.
Video Type	The video protocol used by the archive.
Frame Rate	Specify the media frame rate.
Max Resolution	Specify the maximum resolution that can be used by an endpoint or MCU to connect to the RealPresence Capture Server system for transcoding.
Aspect Ratio	Specify the aspect ratio of the output media file.

Layout	Specify the layout for displaying people and content videos when transcoding dual stream. Users can choose from the following layouts: • **Single window with small content (people 75%; content 25%):** Displays dual stream in one window of which 75% is people video and 25% content video. • **Single window with medium content (people 50%; content 50%)** Displays dual stream in one window of which 50% is people video and 50% content video. • **Single window with large content (people 25%; content 75%):** Displays dual stream in one window of which 25% is people video and 75% content video. • **Single window with people only (content not shown):** Displays people video only in one window with no content. • **Single window with people or content (when content active):** When people and content videos coexist, content video takes priority, people video displays only when content is absent.
Enable VOD Timecode watermarking	Specify whether to enable Timecode (GMT) Watermarking functionality for VoD.
Transfer to Media Server	Specify whether to transfer transcoded media files to external media server.
Snapshot Enable	Specify whether to generate snapshots for transcoded media files.
Enable auto snapshot during entire call	When enabled, snapshots could be generated automatically throughout the entire call.
Start Time	Select the start time for the automatic snapshot.
End Time	Select the end time for the automatic snapshot.
Interval	Set the snapshot interval, measured in second.

4 Click **OK**.

You can click **Save As** to rename the template.

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's IP address or E.164 prefix, default VRR parameters are used for recording. 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

Parameter	Description
VRR Name	Specify a unique name to identify the VRR. You can also use the default name generated by the system.
VRR Number	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.
Description	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.
Recording Template	Specify the recording template. The template defines the basic recording link parameters.
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.
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. Separate several addresses with comma (,).

4. Click **OK**.

   You can click **Save As** to rename the template.

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:

- Calling an interoperable endpoint from RealPresence Capture Server's Admin UI (only for administrators).
- Calling RealPresence Capture Server using an interoperable endpoint's remote control.
- Connecting RealPresence Capture Server to an MCU-hosted call.

Dial out from Capture Server through Admin UI (only for administrators):

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:

Dial Out Parameters

Parameter	Description
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.
Address Type	Specify the address type used to call.
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 Polycom RMX system, you can dial into the conference held on the RMX system 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, select address type as E.164, and dial 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, select address type as H.323 ID, and dial 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, select address type as IP, and dial 172.22.33.44.
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 .
Max Call Rate (Kbps)	Specifies the maximum call rate for the dial-out call.

5. Click **OK**.

Dial out to record is also available under **Call.**
The recording starts immediately if **Start Recording Immediately** is enabled in the selected recording template.
For more information, see Configure VRRs .

Dial in from Endpoint

To start recording by dialing RealPresence Capture Server:

» Enter the E.164 prefix or H.323 ID of RealPresence Capture Server on the remote control of an interoperable endpoint.

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:

- `[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 H.323 ID][VRR number]`

  For example, if the RealPresence Capture Server H.323 ID is `css123`, and the VRR number is 4096, dial *`css1234096`*.

Record from RMX via Recording Link

If you configure the Recording Link function on the Polycom RMX series conference platform and integrate the platform with the RealPresence Capture Server, the RealPresence Capture Server can be called automatically for recording when a multi-point conference is hosted through MCU.

For more information about configuring the Recording Link function on the RMX, refer to the User Guide provided with the RMX system.

Dial into a VRR to Start Recording

You can start recording using a user-defined VRR in one of the following two ways:

- Dialing the VRR through an endpoint.
- Dialing out from VRR using the web Management page to connecting the endpoint.

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.

For VRR format, refer to Dial Out Parameters

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 E.164+VRR@domain format, you need to add SIP Peer to Polycom DMA server, for details, refer to the Polycom DMA server's Administrator's Guide.

To dial in VRR through an endpoint

- If the RealPresence Capture Server system and the endpoint are both registered to a gatekeeper, the dial-in number is [RealPresence Capture Server E.164 suffix][VRR number].

  For example, if the RealPresence Capture Server system's E.164 is 1234 and your VRR number is 1000, you may dial "12341000".
- If the RealPresence Capture Server system and the endpoint are both registered to a SIP server, the dial-in number is [VRR number]@[RealPresence Capture Server IP address].

  For example, if your VRR number is 1000 and the RealPresence Capture Server IP address is 172.21.110.2, you may dial "1000@172.21.110.2".
- If the network is not configured with a gatekeeper, the dial-in number is [RealPresence Capture Server IP address]##[VRR number].

  For example, if the RealPresence Capture Server system's IP address is 172.21.110.2 and your VRR number is 1000, you may dial "172.21.110.2##1000".
- If the network is registered to a SIP server, the dial-in number is [VRR number]@[RealPresence Capture Server IP address].

  For example, if the RealPresence Capture Server system's IP address is 172.21.110.2 and your VRR number is 1000, you may dial "1000@172.21.110.2".

Play Back Media Archives

You can play back recorded media archives stored in RealPresence Capture Server using one of the following methods:

- Playing back from the RealPresence Capture Server system's Admin UI.

  For more information, see Play Back and Download Archives .
- Playing back from RealPresence Capture Server system's Viewer Portal.

  For more information, see Manage Archives and Live Streams Using the Viewer Portal .
- Download recorded files and play back using compatible media players.

  For more information, see Play Back and Download Archives .

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 (version 9.0 or above): From **Tools > Internet Options > Privacy**, make sure the option **Turn on Pop-up Blocker** is NOT selected.

Live Streaming/VoD

You can now stream live meetings (MCU calls) and on demand meeting archives to leading 3rd party media servers, such as Wowza and IIS Media Service (Smooth Streaming only). 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 UI, or from the Viewer Portal.

To stream meetings to an external server, you must first configure the external server, and then select a recording template from VRR.

For more information, see *the Integration Procedure of the RealPresence Capture Server System and Polycom Real Media Management System* from support.polycom.com.

Streaming Using Capture Server

To enable live streaming:

1. Go to **Template > Recording Templates**.
2. Select a recording template.
3. Click **Edit**.
4. Select **Enable Live Streaming**.
5. Click **OK**.

To stream VoDs to an external server:

1. Configure external media servers.
2. Configure a transcoding template.
3. Configure a VRR that uses a transcoding template.

Streaming Using External Servers

To live stream meetings to an external server:

1. Configure external media servers.
2. Add publishing points in **VRR** for external media servers.

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

Parameter	Description
Server Name	Specify the name of the external server.
Server Address	Specify the IP or DNS of the external server you selected.
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

Parameter	Description
Stream Protocol	Choose between **RTSP Steaming** and **RTMP Streaming**.
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.

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.
- You cannot play back IIS media server live streaming and VoD on Android 4.1.2 devices due to Android system limitation.
- Extra latency time will be introduced when external media servers are configured compared with live streaming from the Capture Server system. The exact latency time varies depending on the streaming protocol.

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

Parameter	Description
Application Name	Specify the name of the external media server's application to be used for the VoD. **Note**: Contact the administrator of the external media server for the naming rule of the application name.
FTP Address	Specify the IP or DNS of the external server's FTP server.
FTP Port	Specify the port assigned to the external server's FTP server. The default port is 21.
User Name	Specify your user name to access this FTP server.
Password	Specify your password to access this FTP server.
Default Path	Specify the default FTP directory to save your recordings. Use / to represent the root directory.
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**.

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 720p 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.

Start Live Streaming

Make sure that live streaming has been enabled for the recording template you are using before starting live streaming. For more information, see To define a recording template: .

Procedure for starting a live streaming is the same as the one for starting recording. For more information, see Dial into a VRR to Start 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, and live streaming 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 Viewer 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.

   Note: you can also view live streaming links on **Home** and **Call.**

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. Select a live streaming bitrate.
6. Click Save . Always click **Save** before clicking **OK**; otherwise the entered data will be lost.
7. Click **OK**.

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 configure AKAMAI media server:

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

External Media Servers Parameters

Parameter	Description
Configuration Name	The CONFIG NAME displayed on AKAMAI configuration page under **PUBLISH > Manage Streams**.
Stream Name	The STREAM NAME displayed on AKAMAI configuration page under **PUBLISH > Manage Streams**.
Stream Number	The STREAM ID displayed on AKAMAI configuration page under **PUBLISH > Manage Streams**.
Server Port	Specifies the port that the RealPresence Capture Server system uses to send the encoded MP4 live streams to the AMAKAI server. **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 AKAMAI server, make sure that rules are set to allow the two-way communication between the RealPresence Capture Server system and the AKAMAI server.
Entry Point	Specified on AKAMAI configuration page under **PUBLISH > Manage Streams**.
HDS Playback URL	Specified on AKAMAI configuration page under **PUBLISH > Manage Streams**.
HLS Playback URL	Specified on AKAMAI configuration page under **PUBLISH > Manage Streams**.
User Name	Specify your user name to access the AKAMAI server.
Password	Specify your password to access the AKAMAI server.

4 Click **OK**

This is a charged function and you need an account to log in to the AKAMAI configuration page to get the needed parameters.

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
   - Live Streaming Server:
     - Add
     - Live Streaming Server
     - Publish Point Template
     - Streaming List
   - Email 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 User Guide.
5. Click **OK**.

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.

Archive Details

Parameter	Description
Name	The name of the archive.
Duration	The duration of the archive.
Video Type	The video protocol used by the archive.
Audio Type	The audio protocol used by the archive.
Content Type	The content type of the archive.
Key Words	The keywords for this archive.
Description	Additional user information.

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 generate other media formats.
- **MP4:** MP4 archives (Also known as H.264 streaming files) can be downloaded, such as iPhone and iPad.

- **ISMV:** After the ISMV files are generated, they are uploaded to the IIS Media Server, and can be viewed from the Viewer 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.
- **M4A:** M4A (audio only file) files can be downloaded to PCs, Macs, or to compatible digital media devices, but cannot be viewed from the Viewer Portal.

To play back archives through the Admin UI:

1. Go to **Media > Archives**.
2. Select the archive you want to play back.
3. Click  and the Viewer 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 Manage Archives .

To download one or several archives from Archives page:

1. Go to **Media > Archives**.
2. Select the archive you want to download.

   You can only download archives of the status **Ready**.
3. Click **Download**.
4. Select one or several media types to download.
5. Click **OK**.

To download one or several archives from Media Files:

1. Go to **Media > Archives**.
2. Select the archive you want to download.

   You can only download archives of the status **Ready**.
3. Click **Media Files**.
4. Select one or several media types to download.
5. Click  .

Modify Archives

You can edit archives recorded by your own VRR or 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.

3 If you are authorized to modify the archive, you can modify following parameters:

Archive Properties

Parameter	Description
Name	Specify the name of the archive. **Note:** Only letters, figures, _, space or multi-byte characters can be used for the file name, and the length is 4-20 characters.
Created Time	Specify when the archive was created. **Note:** Created Time cannot be modified.
Description	Specify additional related information.
Enable PIN	Specify whether to enable PIN code protection for the archive.
Key Words	Specify additional information related to the archive.

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

By default, all users are granted permissions to view all archives.

5 Click an item in the list and click **Add**.

6 Click **OK**.

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.**

- Select a transcoding template with lower bit rate, resolution, and frame rate than that of the source file.
- Click **Media > Transcoding** to view the transcoding status.
- Once transcoding is done, find the transcoded files under **Media > Archives.**

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.**

Transcoding

To view media files included in an archive:

1. Go to **Media > Archives**.
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**

Fault Management

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 00:01:00 (GMT) every day. The log file storage is 10GB. You are prompted when the system reaches the storage limit. The system will delete the old logs to free the disk space at 00:01:00 (GMT).

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.
   - Enable SysLog: Specify whether to integrate the system with a syslog server for log collection and management. When a syslog sever is configured, the system forwards its log messages to the server automatically.
   - SysLog Server IP Configuration: To configure the IP settings of the SysLog server.

Auditor Actions

The following table shows actions the auditor can perform.

Auditor Actions

Action	Description
Refresh	Refreshes the list and adds newly generated log files.
Download	Downloads the selected log file.
Download Today's logs	Downloads all the log files generated today.

To download log files:

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

This function is available to administrators and auditors only.

Restart and Shut Down the System

You can shut down or restart your system, or clean the system data and restore it to the factory default configuration.

Before unplugging RealPresence Capture Server, you need to shut down the server in Admin UI.

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.

Upgrade, Backup, Restore, and Migrate

System Upgrade and Downgrade

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.

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 1.6 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. After reboot, delete all temporary IE files, close and restart Internet Explorer.
7. 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.

To downgrade your system software:

1. Go to **Admin > System Upgrade**.
2. Read the terms of the license and agree to them.
3. Click **Open** and select software downgrade package, then click **Upload**.
4. When asked to confirm the action, click **Yes**.

   The system uploads the package and performs the downgrade automatically.

   This may take several minutes.
5. Upon completion of the upload, the system restarts to apply changes.

   This may take several minutes.
6. After reboot, delete all temporary, delete all temporary IE files, close and restart the web browser.

7 Enter your administrator **User ID** and **Password** and then click **Log In**.

To confirm that the system is downgraded, check the software version on the **Product Activation** page.

Backup and Restore

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**
- **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 Data

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

You can also configure FTP servers and transfer meeting recordings to these servers for Video on Demand service.

To configure an FTP server for backup:

1. Go to **Admin > Data Backup/Restore.**
2. Configure the following settings:

FTP Server Parameters

Parameter	Description
Server Address	Enter the IP address of the FTP server.
Port	Enter the port of the FTP server.
User Name	Enter the account and password for login to the FTP server. **Note:** The registered FTP user should possess read-write permissions to user root directory.
Password	
Use Anonymous	When this is enabled, you can log in to the FTP server using anonymous account.
Enable SSL	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.
Test	Test whether the FTP configurations work.

3. Click **Update**.

   When the RealPresence Capture Server system is connected to the FTP server, **Backup/Restore Status** on the page displays **Connected**.

Back Up and Restore Archives

There are two ways to backup archives on the RealPresence Capture Server system to a FTP server:

- **Full backup**.
- **Increment backup:** Files which have been backed up are not backed up again.

To automatically back up archives:

1. Go to **Admin > Data Backup/Restore**.
2. In the **Media backup configuration** area, specify where to save the backup data in the text field beside **Media Back Path**.

3 Select **Enable automatic media backup**.

4 Configure the following settings:

- Frequency: Select the period for automatic backup, measured in day.
- Start Time: Select the start time of automatic backup.

5 Click **Update**. The system restarts to apply your changes.

To back up the archives manually:

» 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.

Manage Archives and Live Streams Using the Viewer Portal

The RealPresence Capture Server provides Viewer Portal for you to view and play archives.

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.

The following tables shows the authorities of each role.

Authorities

Access Privileges	Administrator	User	Auditor	Anonymous access
Access archives	Y	Y	N	Y
View live streaming	Y	Y	N	Y

To log in to the Viewer Portal:

1. Open a web browser.
2. In the browser address line, enter the system's portal address, for example, **http://System IP**

When an IPV6 address is used, a port number must be added. For example:

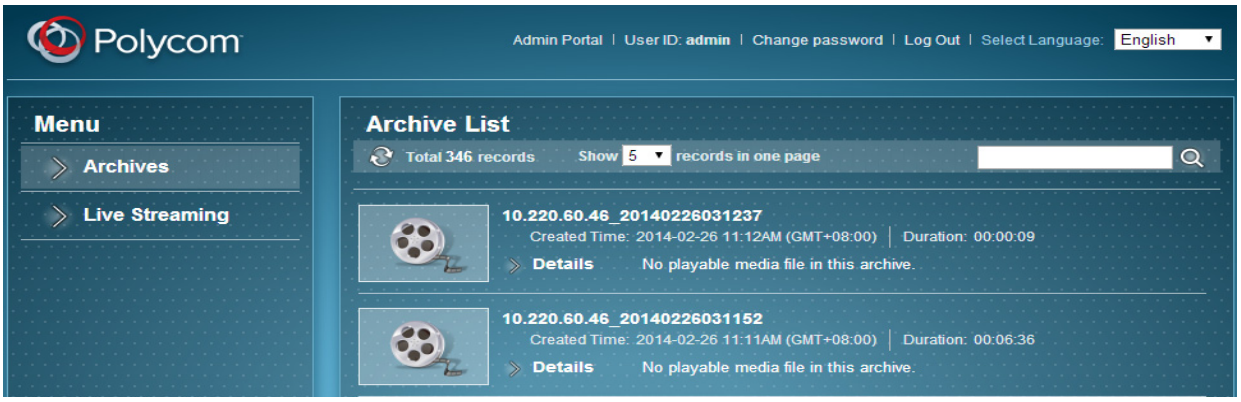
```
http://[ipv6]
http://[ipv6]
```

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**

To switch to the Admin UI from the Viewer Portal:

1. In the address line, enter the system's IP address in this format: http://<system IP address>/.
2. Click **Log In**, and then enter your user name and password to log in to the system.

RealPresence Capture Server Viewer Portal



Manage Archives and Live Streams Using the Viewer Portal

You can view live streaming and play back archives from the Viewer 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.

To view archived files:

» Click **Archives**.

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

To search in archives or live streaming:

1 Click **Archives** or **Live Streaming**.

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 an archived file:

1 Click **Archives**.

2 Click a media file to play it.

The media file is played in a new window.

To view a live streaming recording:

1 Click **Live Streaming**.

2 Click a live streaming to view it.

The live streaming is opened in a new window.

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 Viewer 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 Streams

You can view live streams using one of the following methods:

- View video from the RealPresence Capture Server system's Viewer Portal.

  For more information, see Manage Archives and Live Streams Using the Viewer Portal .
- View video from the Admin Portal of external media servers, if configured.

To view your live streaming from the Viewer Portal:

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

2 In the browser address line, enter the system's portal address, for example, **http://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.

Appendix A – Console Commands

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

Enable Console in Windows

Before you can use Console service to configure your RealPresence Capture Server, you need to configure the application first.

Before you can use Console to configure your system, you need to enable the Console service first. Below is an example on how to enable Console service on Windows 7.0.

To connect with Console:

1. Click the **Start** button. Type *cmd* in the search box.
2. Type *Console* at the command prompt, followed by the IP address of your RealPresence Capture Server.

Login Console

If you have completed all the above configurations and launched Console successfully, press the **Enter** key. The login interface appears.

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.

Console Command Descriptions

You can use the following commands.

Help

After logging into the system, you may enter *?* or help after the prompt # to show the command prompt information.

- “< > ” indicates an optional parameter
- “{}” indicates a required parameter
- “|” indicates a 1-out-of-N parameter

Exit

Enter *exit* after the prompt # to exit the command control interface.

```
# exit
User logged off
```

Viewing Device Information

Enter *show* after the prompt # to view the current device information, including the system information, license information, interface information and IP address.

Reboot Device

Type *reboot* after the prompt # to restart the system. The system will show the prompt message *Are you sure?*. Type *Y* to restart the system, or type *N* to cancel.

```
# reboot


Are you sure reboot now? [Y for yes / N for no]
```

Power off System

Type *shutdown* after the prompt # to power off the system. The system will show the prompt message **Are you sure?**. Type *Y* to proceed, or type *N* to cancel.

```
# shutdown


Are you sure power off now? [Y for yes / N for no]
```

Reset Password

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

Restore System Configuration

Type *reset config* after the prompt # to restore the following system configurations to the default value:

- System Config
  - IP Setting
  - System time
  - Recording Setting

  - Security setting (Ports and security policy)
  - Service Setting
  - Signaling Setting
  - Administrator User Password
- Admin
  - UI Customization (System name and default endpoint menu language)
  - Disk Warning

The system will show the prompt message **Are you sure?**. Type *Y* to proceed, or type *N* to cancel.

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

Check Disk Space Usage

Type *df* after the prompt # to view the disk space usage of RealPresence Capture Server.

The total, used, and free disk space are shown.

Ping

Enter ping <ip > {-n<count > } {-w<time > } {-l<size > } after the prompt # to check the network connection status.

Parameter	Description
ip	IP address of the destination host
-n<count >	Packet sending times, defaulted to 10
-w<time >	Waiting time, defaulted to 1000 ms
-l<size >	Size of the sent packet, defaulted to 32 bytes

[Example] Send the host whose IP address is 172.21.100.111 a Ping packet with the size of 1500 bytes for five times cyclically. The wait time is 1000 ms:

```
# ping 172.21.100.111 -n5 -w1000 -l1500

Pinging 172.21.100.111 with 1500 bytes, loop 5 times, wait 1000 ms.

1520 bytes from 172.21.100.111 : seq=1, ttl=127, delay=1ms.
1520 bytes from 172.21.100.111 : seq=2, ttl=127, delay=2ms.
1520 bytes from 172.21.100.111 : seq=3, ttl=127, delay=2ms.
1520 bytes from 172.21.100.111 : seq=4, ttl=127, delay=2ms.
1520 bytes from 172.21.100.111 : seq=5, ttl=127, delay=1ms.

send 5 packets, receive 5 packets, lost 0(0.0%) packets.
time is 5005ms, bandwidth is 12.1kbps
```

Network Settings

Enter the following commands after the prompt # to set network configurations:

set {lan1 | lan2} ip dhcp - set the DHCP IP address for LAN 1 or LAN 2.

set {lan1 | lan2} ip static {ip} netmask {mask } gw {gateway} - set the IP address for LAN 1 or LAN 2.

set {lan1 | lan2} speed {auto | 1000 | 100 full | 100 half | 10 full | 10 half} - set the duplex speed for the LAN 1 or LAN2 interface.

Parameter	Description
dhcp	Automatically gets the address information through the DHCP server.
static	Specifies the static IP address information - Ip: IP address of the network port mask: subnet mask of the network port gateway: gateway address of the network port

Parameter	Description
auto	Auto negotiation mode
1000	1000Mbps
100 full	100Mbps full duplex
100 half	100Mbps half duplex
10 full	10Mbps full duplex
10 half	10Mbps half duplex

[Example 1] Set the IP address of the LAN1 interface to 172.21.103.29, subnet mask to 255.255.255.0, and the gateway address to 172.21.103.254:

```
# set lan1 ip static 172.21.103.29 netmask 255.255.255.0 gw 172.21.103.254

Reboot is require in order for the change to take effect. Reboot now? [Y for yes
 / N for no]Y

restart system ...
```

[Example 2] Set the 100M half duplex for the LAN1 interface:

```
# set lan1 speed 100 half


Reboot is require in order for the change to take effect. Reboot now? [Y for yes
 / N for no]Y

restart system ...
```

After you set the connection feature or IP address for the LAN interface, the system must be restarted in order for the new settings to take effect.

Appendix B – Configure External Servers

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

- Wowza Media Server
- IIS Media Server

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

Live Stream Meetings to an External Media Server

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

1. Configure the external media server on the RealPresence Capture Server system.
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.

Configure the Wowza Media Server

To configure the Wowza server:

1. Install JDK and Wowza. Run

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

Wowza Media Server Configurations and Directories

Parameter	Live Streaming	VoD
Application Name	live	VoD
Application Directory	<Wowza directory>\applications\live	<Wowza directory>\applications\vod
Configuration File Location	<Wowza directory>\conf\live\Application.xml	<Wowza directory>\conf\vod\Application.xml

2. 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.

3 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.

4 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

Wowza Server Parameter

Parameter	Description
Server Name	Specify the name of your **Wowza Media Server**.
Server Address	Specify the Wowza server IP address.
Server Port	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.

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

Enable Live Streaming

Parameter	Description
Streaming Protocol	Choose between **RTSP streaming** and **RTMP streaming.**
Application Name	Specify the name of the Wowza server application to be used for the live streaming. It should be consistent with the Wowza server configuration. In this example, application name is *live*.
User Name	Specify the user name to access the Wowza media server. This option is required when Wowza authentication is enabled. The **User Name** should be consistent with your input in To configure the Wowza server:

Password	Specify the password to access the Wowza media server. This option is required when Wowza authentication is enabled. The **Password** should be consistent with your input in To configure the Wowza server: .
Test	Test whether the live streaming configurations work.

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

Parameter	Description
FTP Address	Specify the IP address of the Wowza server.
FTP Port	Specify the port assigned to the Wowza server's FTP server. The default port is 21.
User Name	Specify your user name to access this FTP server.
Password	Specify your password to access this FTP server.
Default Path	Specify the default FTP directory to save your recordings. Use / to represent the root directory.
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**.

- 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.
   a. Select *live*.
   b. Double click **Authentication**.
   c. 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. Select *live* and then double click **Live Smooth Streaming Publishing Points**.
4. Right click the **Live Smooth Streaming Publish Points** panel, select **Add** from the context menu to create a new publishing point.
5. In Basic setting, input **File name** and keep other parameters as default value.
6. Click **Advanced Settings**, clear **Archive media**, and check **Start publishing point automatically upon first client request**. Keep other parameters as default value
7. Click **Mobile Devices**, select the **Enable output to Apple mobile digital devices** option, and **set Maximum bit rate (Kbps)** to 5000.
8. Click **OK** to save your settings.
9. 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.

- `clientaccesspolicy.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 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>
```

10 Configure a virtual directory for VoDs if you want to play the archives through an IIS Media server.

11 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`.

12 Install and configure a supported FTP server. The FTP server shares the VoD physical path, for example, `C:\inetpub\wwwroot\vod`.

13 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

Parameter	Description
Server Name	Specify the name of your IIS Media Server.
Server Address	Specify the IIS server IP address.
Server Port	Specify the port that the IIS server used to receive MP4 live streaming. The value is 80 by default. **Note:** 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.

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

Enable IIS for Live Streaming

Parameter	Description
Application Name	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.
User Name	Specify the user name to access the IIS media server. This field is mandatory for Windows authentication on IIS servers.
Password	Specify the password to access the IIS media server. This field is mandatory for Windows authentication on IIS servers.
Test	Test whether the live streaming configurations work.

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

Parameter	Description
FTP Address	Specify the IP address of the IIS media server.
FTP Port	Specify the port assigned to the IIS media server's FTP server. The default port is 21.
User Name	Specify your user name to access this FTP server.
Password	Specify your password to access this FTP server.
Default Path	Specify the default FTP directory to save your recordings. Use / to represent the root directory.
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**.

You cannot create two external servers with the same Server type, IP, Port, Application Name, and Publishing Point 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.

To configure a template and VRR for use with the IIS server, see To create a VRR for use with an external server:

View the Streaming through External Media Server

You can view media files via supported external media servers.

To view media files:

1 In the browser address line, enter the system's portal address, **http://System IP.**
2 Click **Log In** at the upper right of the screen.
3 To view a live streaming, click **Live Streaming** and select the desired streaming.
4 To view a streaming on demand, click **Archives** and select the desired streaming.

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 for 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 for H.323 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 HDX 4000 to the VCS.

Now you can dial from the HDX 4000. 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 UI.

Configure VCS for SIP Calling

If your network supports SIP, you can use SIP to connect IP 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.

c Configure the zone for your RealPresence Capture Server. Refer to the following table.

VCS Zone Parameters

Parameter		Settings
Name		capture_server_zone
Type		Neighbor
Hop count		15
H.323	Mode	On
	Port	1719
SIP	Mode	On
	Port	5060
	Transport	TCP
	Accept proxied registration	Allow
Authentication policy		Do not check credentials
SIP authentication trust mode		Off
Peer 1 address		Your RealPresence Capture Server IP address.
Zone profile		Custom

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

Parameter	Settings
Rule name	captureserverroute
Description	Route for RealPresence Capture Server
Priority	3
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	(99\d+)@*RealPresence Capture Server IP* **Note**: This string allows you to call only VRRs that start with the number 99, for example, 9912345@172.21.124.104. You can change the pattern string according to your situation.
Pattern behavior	Replace
Replace string	\1
On successful match	Stop
Target	captureserverzone It points out the zone that you created.
State	Enabled

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 9912345, you can dial *9912345@RealPresence Capture Server IP* directly to start a recording.