ADMINISTRATOR GUIDE

Software 1.7.0 | April 2015 | 3725-03273-005D

RealPresence® CloudAXIS® Suite

Copyright© 2015, 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.

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.

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

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

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. E-mail your opinions and comments to DocumentationFeedback@polycom.com.

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

Contents

Conventions Used in Polycom Guides **7**

Information Elements 7
Typographic Conventions 7

Before You Begin **9**

Terminology Used in this Guide 9
RealPresence CloudAXIS Services and Experience Portals 10
The RealPresence Platform 10
RealPresence CloudAXIS Suite Components *11*
RealPresence Platform Components *11*
Ports and Protocols *13*
Setup Worksheets 15
Start and Restart Order for RealPresence CloudAXIS Suite Components 21
Start RealPresence CloudAXIS Suite Components *21*
Restart RealPresence CloudAXIS Suite Components *21*
Get Help 21
Polycom and Partner Resources *21*
The Polycom Community *22*

Get Started **23**

Deploy RealPresence CloudAXIS Suite Software Packages 23
*Deploy the *.OVA Packages* *23*
*Deploy the *.VHD Packages* *24*
Verify that Both Portals are Accessible 25
Open the RealPresence CloudAXIS Services Portal *26*
Open the RealPresence CloudAXIS Experience Portal *26*
Set Up RealPresence CloudAXIS Suite for the First Time 27
Configure Network Settings 27
Assign IP Addresses for Both Portals *27*
Modify Settings in your DNS Server *28*
Set the Time Zone and NTP Server *28*
Verify the Time Settings *28*

Manage Trust Certificates and Certificate Signing Requests **30**

Generate Certificates and Certificate Signing Requests 30
View Certificates 32
Copy a CSR 32
Delete Certificates 33
Upload Certificates or a Certificate Chain 33
Configure Certificates for Reverse Proxy *35*

RealPresence CloudAXIS Services Portal Server Settings 36

Set Web Addresses for RealPresence CloudAXIS Portals 36
Select a User Authentication Mode 37
Set Up LDAP Authentication 37
Set Up Single Sign-On Authentication 38
Enable E-mail Notifications for Users 42
Set Social Networking Policies 43
Enable Social Networking Contacts 43
Disable Social Networking Contacts 44
Connect to a Polycom Access Point 44
Add a RealPresence DMA System and Access Points 45
Change an Existing RealPresence DMA Connection 47
Set Conference Preferences 47
Add a Language Pack 48
Customize E-mail Templates 49
HTML Variables Used in E-mail Templates 50
Reset an E-mail Template 52
Customize and White Label the User Interface 53
Customize the User Interface 53
Change the Login Screen Display 54
Add a Notification Message for Users 54
Add a Logout URL 55
Add a Footer to the User Interface 55
Refresh Custom User Interface Settings 55

RealPresence CloudAXIS Services Portal Platform Settings 57

Set the Server Date and Time 57
View and Download Logs 57
Update RealPresence CloudAXIS Services Portal Software 59
Migrate Current Settings to the New RealPresence CloudAXIS Services Portal 59

Monitor the RealPresence CloudAXIS Environment 61

SNMP Framework 61
Polycom Use of SNMP 61
SNMP Notifications 62
Enable and Configure System Monitoring 63

User Management 67

Account Roles 67
Manage User Accounts 68
Change System Administrator Password 68
Create User Accounts 68
Edit User Accounts 70
Delete User Accounts 71
Reset User Passwords 71

RealPresence CloudAXIS Experience Portal Conference Settings 73

Set the Experience Portal Web Addresses 73
Configure Conference Authentication Settings 74
Set Authentication Rules 74
Configure Services Portal Authentication 75
Configure Conference Rules and Settings 76
Set Conference Lobby Rules 76
Configure the DMA Agent 77
Configure the VMR Agent and VMR Conference Settings 78
Configure the Services Portal Conference Agent and Conference Settings 81
Add Language Packs to the RealPresence CloudAXIS Experience Portal 82
Manage User Roles 82
User Roles and Permissions 83
Roles Assignment 84

RealPresence CloudAXIS Experience Portal Platform Settings 86

Set the Server Date and Time 86
Assign an IP Address to the Server 86
Manage RealPresence CloudAXIS Experience Portal Log Files 87
Set the Log Level 87
Download and View Log Files 88
Clear Log Files 88
Update RealPresence CloudAXIS Experience Portal Software 88
Export Current RealPresence CloudAXIS Experience Portal Settings 89
Import Settings to a New RealPresence CloudAXIS Experience Portal 89
Restart the CloudAXIS Experience Portal Services or Server 90
Restart the RealPresence CloudAXIS Experience Portal Services 90
To Reboot the Server 90

Activate RealPresence CloudAXIS Suite Licenses 91

Activate RealPresence CloudAXIS Suite Licenses within Platform Director 91
Set Up Licensing on the RealPresence CloudAXIS Services Portal 91
Set Up Licensing on the RealPresence CloudAXIS Experience Portal 93
Allocate Licenses for RealPresence CloudAXIS Suite 94
View RealPresence CloudAXIS Suite License Status 94
Activate Licenses for a Stand-Alone RealPresence CloudAXIS Suite 95
Activate Licenses in Online Mode 95
Activate Licenses in Offline Mode 97
Activate the RealPresence Experience Portal Connection 98
Deactivate Licenses 98

Secure Shell and Restricted Shell Commands 101

Recommendations for Secure Access 104

Secure Web Access 104
Tunnel Access for Remote Users 104

Limitations Associated with Tunneling *105*
Secure SIP Access for Guests 106
Edge Proxy Access for Guests *106*
Additional Recommendations to Increase Security *107*

Troubleshoot Issues **108**

Appendix 1: Set Up Windows Active Directory for Single-Sign-On **113**

Create a RealPresence CloudAXIS Services Portal User Account in Active Directory 113
Set a Service Principal Name for the Services Portal User Account in Active Directory 114
Generate a Keytab File for the Services Portal User 114

Appendix 2: Create Apps to Use with Social Media Contacts **116**

Create a Google+ Application 116

Appendix 3: Cookies Used by the Applications **120**

Appendix 4: DMA Factory Conference Settings Impact **121**

Conventions Used in Polycom Guides

Polycom guides contain graphical elements and a few typographic conventions. Familiarizing yourself with these elements and conventions will help you successfully perform tasks.

Information Elements

Polycom guides may include any of the following icons to alert you to important information.

Icons Used in Polycom Guides

Name	*Icon*	*Description*
Note		The Note icon highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.
Administrator Tip		The Administrator Tip icon highlights techniques, shortcuts, or productivity related tips.
Caution		The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.
Warning		The Warning icon highlights an action you must perform (or avoid) to prevent issues that may cause you to lose information or your configuration setup, and/or affect phone, video, or network performance.
Web Info		The Web Info icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.
Timesaver		The Timesaver icon highlights a faster or alternative method for accomplishing a method or operation.
Troubleshooting		The Troubleshooting icon highlights information that may help you solve a relevant problem or to refer you to other relevant troubleshooting resources.
Settings		The Settings icon highlights settings you may need to choose for a specific behavior, to enable a specific feature, or to access customization options.

Typographic Conventions

A few typographic conventions, listed next, are used in Polycom guides to distinguish types of in-text information.

Typographic Conventions

Convention	*Description*
Bold	Highlights interface items such as menus, menu selections, window and dialog names, soft keys, file names, and directory names when they are involved in a procedure or user action. Also used to highlight text to be entered or typed.
Italics	Used to emphasize text, to show example values or inputs (in this form: <*example*>), and to show titles of reference documents available from the Polycom Support Web site and other reference sites.
Blue Text	Used for cross references to other sections within this document and for hyperlinks to sites and documents external to Polycom such as third-party web sites, documentation, and support.
Blue Text in italics	Used for hyperlinks to external Polycom resources such as Polycom Support and product web pages.
`Courier`	Used for code fragments and parameter names.

Before You Begin

The Polycom® RealPresence® CloudAXIS® Suite enhances the Polycom® RealPresence® Platform by providing access to a shared meeting and collaboration experience that can include users from the hosting organization and guests from outside the organization. The suite includes two virtualized server components: the RealPresence CloudAXIS Services Portal and the RealPresence CloudAXIS Experience Portal. This guide shows you how to deploy, configure, and manage both portal packages and create and manage user accounts.

Web Info: An Online Version of this Document is Available

Note that if you are reading this document in PDF format, an online version of the *Polycom RealPresence CloudAXIS Suite Administrator Guide* is available on the Polycom Technet web site.

Terminology Used in this Guide

As you read this guide, you will notice some terms and conventions used repeatedly. Familiarize yourself with these terms and conventions so you understand how to perform administration tasks.

Terms Used in this Guide

Term	*Definition*
Apache Tomcat	An open-source web server and application container that runs the RealPresence CloudAXIS Services Portal application.
RealPresence CloudAXIS Experience Portal	The meeting conference interface, which is referred to in the user interface as the Meeting Experience Application or the Meeting Portal in the *RealPresence CloudAXIS Suite User Guide*.
FQDN	The acronym for Fully Qualified Domain Name. An example of an FQDN is dma.example.com.
Network Time Protocol Server (NTP)	The NTP server sets the time and date settings for the RealPresence CloudAXIS Services Portal.
Nginx	An HTTP server used to render static content and delegate requests to Apache Tomcat.
RealPresence CloudAXIS Services Portal	The back-end, web server component of RealPresence CloudAXIS Suite that handles scheduling meetings, adding users, and adding contacts. It is referred to in the user interface as the Web Services Portal or the Web Portal in the *RealPresence CloudAXIS Suite User Guide*.
Virtual Edition	Designates that a RealPresence CloudAXIS Suite component is a software-based virtual machine.

Term	*Definition*
Virtual meeting room (VMR)	A virtual meeting space that users and endpoints can join to participate in a multi-party videoconference. VMRs are identified and addressed by numeric IDs. A VMR may be personal or temporary. A personal VMR (also known as a persistent VMR) remains in existence indefinitely and can be used for different individual meeting events over time. A temporary VMR is created for a specific meeting or time period and is deleted once the meeting or time period has ended. See the *Polycom DMA 7000 System Operations Guide* for more information on VMR management.
VMR prefix	Specifying a VMR prefix value allows the RealPresence CloudAXIS Services Portal and the RealPresence CloudAXIS Experience Portal to know where to direct requests concerning a particular VMR ID. For example, if DMA-1 had the dialing prefix specified as 1, and DMA-2 had no dialing prefix specified, all portal requests concerning VMRs with ID 1xxxx would be directed to DMA-1, and requests concerning any other VMR ID would be directed to DMA-2.

RealPresence CloudAXIS Services and Experience Portals

Through the RealPresence CloudAXIS Services Portal, users create and participate in online video conference meetings. Users create meetings by logging into the RealPresence CloudAXIS Services Portal, selecting the type of meeting they want to create, setting the meeting parameters, and entering a list of participants to invite. In RealPresence CloudAXIS Services Portal, administrators can create and manage users and configure the components for online video conference meetings.

In the RealPresence CloudAXIS Experience Portal, users attend meetings and interact with features such as content sharing, group chat, and privacy settings.

The RealPresence Platform

This section describes the RealPresence Platform, lists the deployment requirements, and provides worksheets that help you deploy and configure the RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal. When you have completed the worksheets and are ready to deploy and configure the RealPresence CloudAXIS Services Portal, see Get Started.

The Polycom RealPresence Platform product suite enables standards-based videoconference collaboration between hardware and software endpoints from Polycom and other optional vendors. This implementation may include one or more of the components listed in the following table.

RealPresence Platform Components

Required or Optional	*Polycom Platform Component*	*Purpose*
Required	Polycom® RealPresence® Distributed Media Application™ (DMA®), Virtual Edition	Signaling, call control, and bridge virtualization
Required	Polycom® RealPresence® Collaboration Server (RMX®), Virtual Edition	Multipoint Control Unit (MCU) for hosting conferences

Required or Optional	*Polycom Platform Component*	*Purpose*
Optional	Polycom® RealPresence® Resource Manager	Provisioning and managing endpoints
Optional	Polycom® RealPresence® Access Director™ solution*	Firewall traversal
Optional	RSS™ recording and streaming server	Media recording
Optional	Polycom® RealPresence® Capture Server	Media recording

*An Acme Packet Net-Net Enterprise Session Director may also be used to secure firewall traversal.

RealPresence CloudAXIS Suite Components

The RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal interoperate with RealPresence Platform components, along with the following standard IT infrastructure elements provided by the deploying organization. The component list that follows is also illustrated in the accompanying figure.

Primary infrastructure components of a RealPresence CloudAXIS Suite environment are listed in the following table.

Infrastructure Components

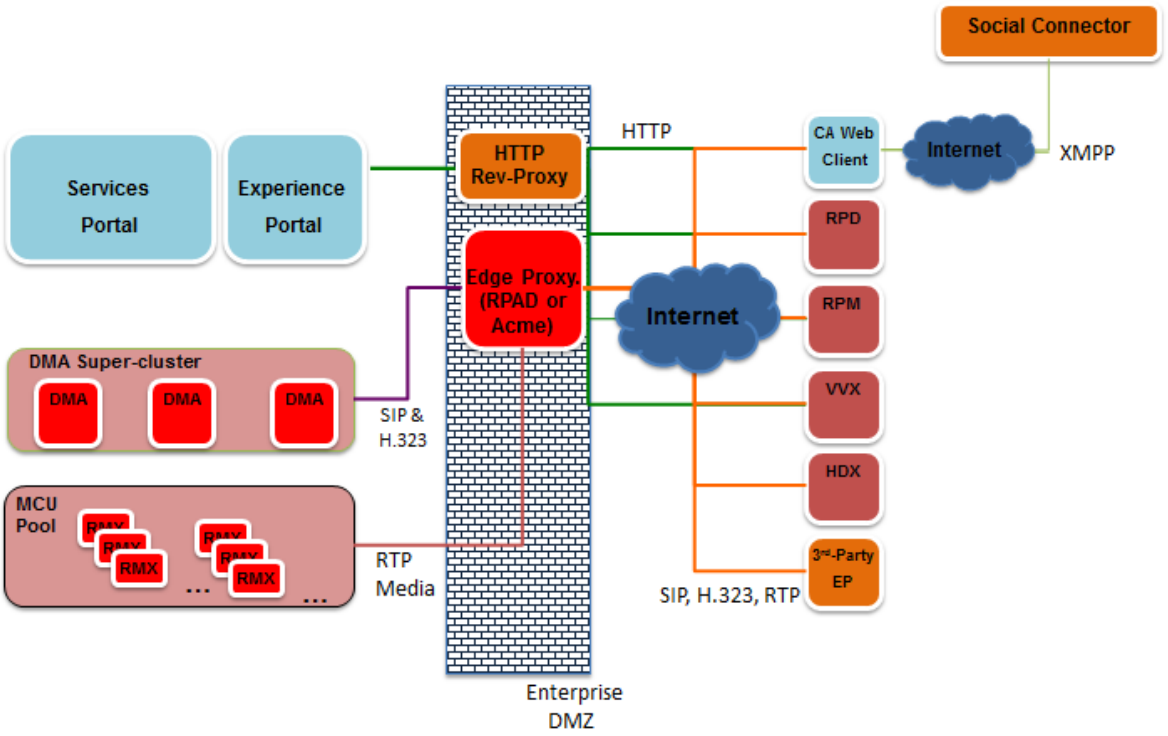
Component	*Description*
Dynamic Host Configuration Protocol (DHCP) server	Assigns IP addresses to portal components and devices.
Domain Name System (DNS) server	Allows the portals and other RealPresence Platform components to be found and referenced using domain names rather than IP addresses.
Lightweight Directory Access Protocol (LDAP) server	Allows the portals to be integrated with an LDAP-compatible directory (for example, a Microsoft Active Directory server) to facilitate user management and authentication.
Simple Mail Transport Protocol (SMTP) server	Enables the sending of meeting invitations and other user notifications, including login information and password resets and updates, via e-mail.
HTTP Reverse Proxy Server	Allows web access to the RealPresence CloudAXIS portals from outside the organizational firewall. For more information, see Secure Web Access.

RealPresence Platform Components

The following diagram shows the components required for the RealPresence CloudAXIS Services and RealPresence CloudAXIS Experience Portals in the RealPresence platform. The diagram is color-coded as follows:

- **RealPresence CloudAXIS components** Identified by light blue.
- **Third-Party components** Identified by orange.
- **RealPresence components** Identified by bright red.
- **Endpoints** Identified by dark red.

Polycom RealPresence Platform components



RealPresence Platform components work with the RealPresence CloudAXIS Suite to enable users to create and participate in video conference meetings using a web browser or other hardware and software video endpoints, including mobile devices running the Polycom® RealPresence® Mobile application.

If Polycom RSS or Capture Server is configured for the environment that is hosting the meeting, the creator of the meeting can record it, including all video streams, audio streams, and shared content.

The RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal

Meetings are scheduled in the RealPresence CloudAXIS Services Portal and attended through the RealPresence CloudAXIS Experience Portal. The RealPresence CloudAXIS Suite portals can run on one or more VMware ESXi 5.x hosts or be deployed as virtual machines using Microsoft® Hyper-Visor (Hyper-V) Server 2012 R2. Scheduling a meeting in the RealPresence CloudAXIS Services Portal requires user or administrative account access (see Account Roles). Participating in meetings requires access only to the RealPresence CloudAXIS Experience Portal using a downloaded plug-in and a URL link sent in an e-mail or instant message.

RealPresence CloudAXIS Suite Users

You can add users to the RealPresence CloudAXIS Services Portal locally or through integration with an enterprise Lightweight Directory Access Protocol (LDAP) server. With LDAP enabled, enterprise users can attend and host meetings on the RealPresence CloudAXIS Services Portal and log into the RealPresence CloudAXIS Experience Portal using their domain network credentials.

RealPresence CloudAXIS Suite Meetings

Users log in to the RealPresence CloudAXIS Services Portal, select the Schedule option, choose meeting options, select the participants they want to invite, and then schedule a meeting. The RealPresence CloudAXIS Services Portal then contacts the RealPresence DMA system to create a virtual meeting room (VMR) on a multipoint control unit (MCU) where all participants can join. Finally, the configured Simple Mail Transfer Protocol (SMTP) server sends the e-mail notifications to each invited participant. The invitation contains a URL link to the meeting and can include information for how to access meetings using SIP, H.323, ISDN, Tunneling, or PSTN. When the meeting takes place, the RealPresence DMA system validates the VMR and routes the call to the destination RealPresence Collaboration Server (RMX) so that users can join. When a user creates a meeting that starts immediately (an ad hoc meeting), a RealPresence CloudAXIS Experience Portal session opens and prompts the user to begin inviting participants.

RealPresence CloudAXIS Suite Meeting Contacts

Users can invite participants to meetings from an aggregated list of the meeting creator's Google+ contacts if the RealPresence CloudAXIS Services Portal administrator has enabled and provisioned app-user credentials on the relevant service. If social media contacts are enabled, a user can invite social networking contacts to meetings that occur on the RealPresence CloudAXIS Experience Portal.

When a contact is selected in the Services Portal, a URL is sent to the contact on that social messaging service. The invited participants can click the URL or paste it in to their browser to gain access to the meeting.

RealPresence CloudAXIS Suite System Deployment

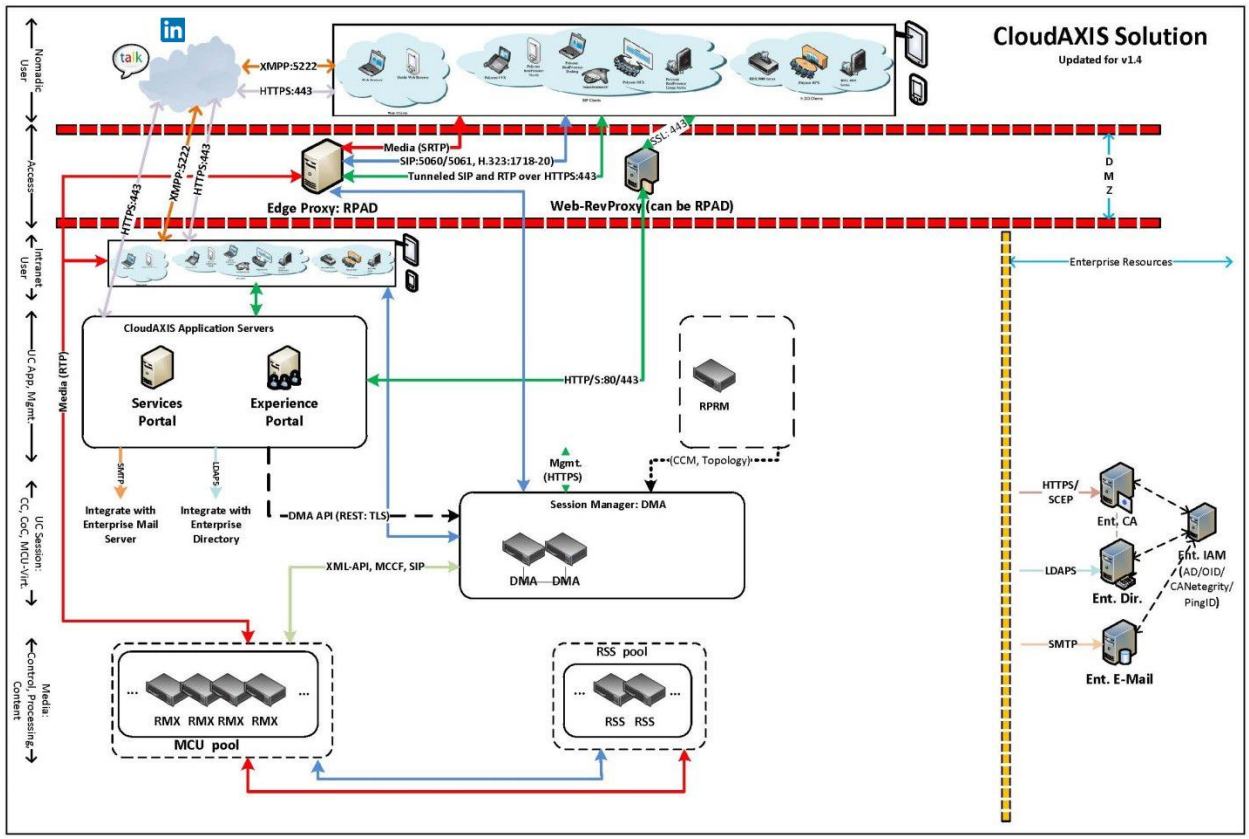
The RealPresence CloudAXIS Services Portal and the RealPresence CloudAXIS Experience Portal are each packaged in OVA files that can be deployed on VMware ESXi hosts using vSphere tools (for example, VMware vCenter using the vSphere client). Both portals are also packaged in VHD files that can be deployed as virtual machines on Microsoft Hyper-V server.

Ports and Protocols

This section illustrates and describes the ports and protocols that ensure successful network traversal for the RealPresence CloudAXIS Services Portal. Inbound and outbound port usage depends on the communications protocol and the specific port being used to initiate communications.

The following graphic shows how various ports and communications protocols interact in a sample RealPresence CloudAXIS Suite network.

Ports and protocols used in the RealPresence CloudAXIS Services Portal



The following table describes the inbound and outbound ports and protocols that handle communications between the RealPresence CloudAXIS Services Portal and other Polycom RealPresence system components.

Inbound and Outbound Protocols and Ports

Protocol/Function	*Communication*	*Inbound Ports*
HTTP/HTTPS	From web clients to the RealPresence CloudAXIS Services and RealPresence CloudAXIS Experience Portals	TCP 443. Port 80 is also enabled, but it redirects to 443. Provides web browser access to the User Interface (UI) and Representational State Transfer (REST) APIs.
HTTPS	Between the RealPresence CloudAXIS Experience Portal and the RealPresence DMA system	TCP 8443 from Experience Portal to RealPresence DMA system TCP 9443 from RealPresence DMA system to Experience Portal
HTTPS (Tunneling)	From web clients to RealPresence Access Director (version 3.1 is required to set up tunneling in a RealPresence CloudAXIS Suite environment)	TCP 443. Port 80 is also enabled, but it redirects to 443. Media is communicated through RealPresence Access Director.

Protocol/Function	*Communication*	*Inbound Ports*
SMTP	Between the RealPresence CloudAXIS Services Portal and the organization's SMTP server	TCP 25 for non-secure (SMTP). TCP 587/465 for secure (SMTP-S).
LDAP	Between the RealPresence CloudAXIS Services Portal and the organization's LDAP server	TCP 389 for non-secure (LDAP). TCP 636 for secure (LDAP-S).
Extensible Messaging and Presence Protocol (XMPP)	Between web clients and external social media services	TCP 5222. The RealPresence CloudAXIS Services Portal uses this port to communicate with social networking apps to get contact presence information and deliver instant message invites.
SIP	Between client endpoints and RealPresence DMA system or the intermediate Edge Proxy (Polycom® RealPresence® Access Director™ (RPAD) or Acme)	5060 (UDP/TCP) /5061 (TLS). 443 (TCP) for HTTPS Tunneling. SIP is the signaling protocol used by the RealPresence CloudAXIS Suite web client, RealPresence Mobile, and other SIP endpoints.
Real-time Transport Protocol/Real-time Control Protocol/Secure Real-time Transport Protocol/Secure Real-time Control Protocol (RTP/RTCP/SRTP/SRTCP)	Between client endpoints and the MCU or the intermediate Edge Proxy (RPAD or Acme)	RealPresence CloudAXIS Suite web client: UDP ports 3230–3237. 443 TCP port for HTTPS Tunneling. For the RTP/RTCP/SRTP/SRTCP port range used by other Polycom and third-party products, see the appropriate product documentation. RTP and SRTP are used to carry visual and audio media between web-based clients and the RMX. RTCP and SRTCP provide out-of-band statistics and control information for an associated RTP or SRTP flow.
Binary Floor Control Protocol (BFCP)	Between client endpoints and the MCU or the intermediate Edge Proxy (RPAD or Acme)	3238 (UDP/TCP) BFCP is the signaling protocol used by SIP clients to negotiate content sharing.

Setup Worksheets

Before you begin the RealPresence CloudAXIS Services Portal deployment, complete the fields in the My System Values column of each of the Setup Worksheets that follow. Use the information in these worksheets to help you configure the RealPresence CloudAXIS Services Portal.

Setup Worksheet for the LDAP Server Configuration

LDAP Options	*My System Values*	*Description*
Forest Root Domain		The forest root domain name for the company, for example *polycom.com* or *Microsoft.com*.
Secure		Establishes a secure connection to the LDAP server. Note: If Secure is selected, upload the trust certificate of the LDAP server in the RealPresence CloudAXIS Services Portal. See Upload Certificates or a Certificate Chain.
Port		The numerical value of the port through which LDAP communicates. Commonly used values include • 389 for non-secure (LDAP) • 636 for secure (LDAP-S)
Username		The LDAP service account user ID.
Password		The login password for the service account user ID.

Setup Worksheet for the SMTP Server Configuration

SMTP Options	*My System Values*	*Description*
Server		Enter the FQDN or IP address of the SMTP server.
Secure		Select to establish a secure connection to the SMTP server.
Port		After deployment, enter the port to use to connect to the SMTP server. Here are typical values: • 25 for non-secure (SMTP) • 587/465 for secure (SMTP-S)
Login ID		After deployment, enter the SMTP service account user ID.
Password		Enter the login password for the service account user ID.
Sender Mail ID		Enter the e-mail ID to be used as the return address for notifications sent by the RealPresence CloudAXIS Services Portal. This is typically be configured as a null or no reply address.

Setup Worksheet for the Server Settings

Server Settings	*My System Values*	*Description*
RealPresence CloudAXIS Experience Portal (MEA) Server	https://	Enter the URL, including the FQDN assigned to the IP address of the RealPresence CloudAXIS Experience Portal. (See Open the RealPresence CloudAXIS Experience Web Portal.) This information is used to construct the meeting links. Make sure that this domain name is accessible to all users of the solution, including any users that may be located outside of the organization.
RealPresence CloudAXIS Services Portal (WSP) Server	https://	Enter the URL including the FQDN assigned to the IP address of the RealPresence CloudAXIS Services Portal. (See Open the RealPresence CloudAXIS Services Web Portal.) This domain name is used in constructing the login link to RealPresence CloudAXIS Services Portal. Make sure that this domain name is accessible to all users who can access the RealPresence CloudAXIS Services Portal.

Setup Worksheet for the DMA Configuration

System Configuration Information	*My System Values*	*Description*
Name		Enter a nickname to assign to the RealPresence DMA system to distinguish it in the RealPresence CloudAXIS Services Portal configuration.
Host		Enter the FQDN or IP address of a single node RealPresence DMA system, or the virtual IP address or virtual FQDN of a RealPresence DMA system super node.
Port		Enter the TCP port number to use when communicating with the RealPresence DMA system. The commonly used port is 8443, which corresponds to the HTTPS REST API for the RealPresence DMA system.

System Configuration Information	*My System Values*	*Description*
VMR Prefix		Enter the VMR prefix that corresponds to this RealPresence DMA system. This is optional and for use in environments where dialing plans are used to assign different VMR IDs to be handled by a peered set of RealPresence DMA systems. Specifying this value allows the portals to know where to direct API requests concerning a particular VMR ID. For example, if DMA-1 had the dialing prefix specified as *1* and DMA-2 had no dialing prefix specified, all portal requests for VMRs with ID *1xxxx* would be directed to DMA-1 and requests concerning any other VMR ID would be directed to DMA-2. Note that the VMR prefix must match what is on the RealPresence DMA system. To set up this value, see the *Polycom DMA 7000 System Operations Guide*.
Default Admin		Enter a user account name with an administrative role that exists on the RealPresence DMA system. Note that if the RealPresence DMA system is configured to have multiple domains, make sure that the admin user account has access to all the domains and hence can search the VMRs of all users. This typically requires a domain account rather than a local DMA account. See the *Polycom DMA 7000 System Operations Guide* for more details.
Admin Password		Enter the password value defined on the RealPresence DMA system for the Default Admin account.
Owner Domain		Enter the domain of the user account assigned for creating meetings in the RealPresence DMA system. For local domains, enter **LOCAL**.
Common SIP Username		(Optional) Enter a username to use to authenticate SIP sessions for users who have authenticated with the RealPresence CloudAXIS Services Portal.
Common SIP Password		(Optional) Enter a password to use in conjunction with the Common SIP Username to authenticate SIP sessions for users who have authenticated with the RealPresence CloudAXIS Services Portal.

System Configuration Information	*My System Values*	*Description*
Owner Username		Enter the username assigned for creating meetings in the RealPresence DMA system. The username must match the name of a user account defined on the RealPresence DMA system. The user does not need to be an administrator. For information on how to create a username for the RealPresence DMA system, see the *Polycom DMA 7000 System Operations Guide*.
Generate VMR From Range		Selecting the check box displays two text boxes for entering a range. This option is used by administrators to allow the Services Portal to generate VMR IDs on the RealPresence DMA system randomly within a specified range. This allows administrators to separate the temporary VMRs created specifically for RealPresence CloudAXIS meetings from other VMRs on same the RealPresence DMA system. Note that the range must be all positive numbers with a 10-digit maximum. The first text box is for the lowest number of the range and the second text box is for the highest. For example, if entering a range of 123 to 1234, the RealPresence CloudAXIS Services Portal generates VMRs between 123 and 1234.

Setup Worksheet for the DMA Server Access Point Configuration

System Configuration Information	*My System Values*	*Description*
Location		Enter the location name assigned in the RealPresence CloudAXIS Services Portal to identify a particular access point available for dialing. A single location may have multiple transport protocols configured for it. Note that an access point is a network location that is routed directly or indirectly to the RealPresence DMA system from where clients or endpoints can connect to participate in a conference.

System Configuration Information	*My System Values*	*Description*
Transport		Select the transport protocol associated with the location and dial string. Select from SIP, H.323, TUNNEL, ISDN, and PSTN. For information on provisioning endpoints for SIP, see the *Polycom RealPresence Resource Manager Operations Guide*. For information on enabling SIP calls for mobile apps, see the help files on the Polycom RealPresence Mobile Support page. Note: It is mandatory that the RealPresence CloudAXIS Experience Portal have at least one SIP AP configured.
Dial string		Dial strings (SIP URI, Tunnel URI, H.323 E.164 enum, PSTN phone number) are used by a video or audio endpoint to join a conference hosted by the RealPresence DMA system. Typically for SIP, TUNNEL, and H.323 callers, this string includes the address or domain name (preferred) of the edge traversal device (RPAD or Acme) provisioned to allow external access to this RealPresence DMA system.
Auth Mode		Options for this drop-down menu include AUTH, NoAUTH, and SHARED. • For an access point that may be used by endpoints without access to SIP credentials, select **NoAUTH**. • For an access point that is used by endpoints that have access to SIP credentials (for example, authenticated web and RPM client users when the RealPresence DMA system settings have been configured with the Common SIP Username and Password as described), select **AUTH**. • For an access point that may be used by either class of endpoints, select **SHARED**.
Dial Prefix (Optional)		Use this field to specify a prefix to add to dialing information used when dialing this access point. This prefix can be used by the access point to route the call or to distinguish between authenticated callers and unauthenticated guests.

Setup Worksheet for the Date Time Configuration

System Configuration Information	*My System Values*	*Description*
NTP Server		Enter the Network Time Protocol server FQDN or IP address. The RealPresence CloudAXIS Services Portal synchronizes time and date settings from this server. Entering the NTP automatically populates the Date and Time fields. Note that the portals are configured to the UTC time zone.

Start and Restart Order for RealPresence CloudAXIS Suite Components

The following sections describe the order for starting and restarting RealPresence CloudAXIS Suite components.

Start RealPresence CloudAXIS Suite Components

When you start RealPresence CloudAXIS Suite, make sure to start the RealPresence CloudAXIS Services Portal and the configured RealPresence DMA system before starting the RealPresence CloudAXIS Experience Portal. If you do not start RealPresence CloudAXIS Suite in this order, it will impact the API that handles feature functionality on the Experience Portal.

Restart RealPresence CloudAXIS Suite Components

When you restart the RealPresence CloudAXIS Services Portal or the configured RealPresence DMA system, make sure to also restart the RealPresence CloudAXIS Experience Portal afterwards (see Restart the CloudAXIS Experience Portal Services or Server). If you restart the Services Portal or RealPresence DMA system without restarting the Experience Portal afterwards, it will impact the API that handles feature functionality on the Experience Portal.

Get Help

For more information about installing, configuring, and administering Polycom products, refer to Documents and Downloads at Polycom Support.

Polycom and Partner Resources

To find all Polycom partner solutions, see Strategic Global Partner Solutions website.

The Polycom Community

The Polycom Community gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

Get Started

The RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal require deployment on a VMware EXSi host using a vSphere Client administrative GUI. You can also deploy the portals as virtual machines on the Microsoft Hyper-V server. We recommend deploying the RealPresence CloudAXIS Services Portal first and the RealPresence CloudAXIS Experience Portal second.

This section shows you how to deploy both portals and set them up in your virtual network. If you are upgrading RealPresence CloudAXIS from a previous version, this section shows you how to export the configuration from your current environment and upload it into the newly deployed virtual machine environment for both the Services Portal and Experience Portal. If this is your first time installing RealPresence CloudAXIS Suite, this section also lists the tasks you must complete to set up a RealPresence CloudAXIS Services Portal and a RealPresence CloudAXIS Experience Portal for basic operation.

Before you begin, complete the Setup Worksheets and confirm that your system meets all requirements and includes all prerequisites listed in the most current *Release Notes* for the RealPresence CloudAXIS Services Portal and Experience Portal.

Deploy RealPresence CloudAXIS Suite Software Packages

RealPresence CloudAXIS Services Portal and RealPresence Experience Portal installation packages are delivered as VMWare Open Virtual Appliance (OVA) files and Virtual Hard Drive (VHD) files. This section provides information on deploying the portals as virtual machines using the OVA or VHD files.

Deploy the *.OVA Packages

You can deploy the RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal as a virtual machine using the OVA files and following the VMWare deployment procedures.

The following instructions show how to deploy the *.OVA packages outside a RealPresence Platform Director environment.

To deploy the *.OVA packages in your VMWare environment:

1. Confirm that your system includes the prerequisites and meets the requirements listed in the Release Notes for the version of the RealPresence CloudAXIS software that you are deploying.
2. Download the appropriate *.OVA files from the Polycom RealPresence CloudAXIS Support site.
3. Using the vSphere client on your vSphere EXSi host server, deploy the *.OVA files for the RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal into your VMWare environment.

You can also deploy the RealPresence CloudAXIS Services Portal and Experience Portal within a Polycom® RealPresence® Platform Director instance that has been deployed in your organization's VMware environment. See the *RealPresence Platform Director Administrator Guide* for instructions on how to add instances of component RealPresence products to an existing RealPresence Platform Director instance.

To deploy the CloudAXIS *.OVA files within a Platform Director Environment, see the *RealPresence Platform Director Administrator Guide*. It includes instructions for deploying both new and existing instances of RealPresence component products including RealPresence CloudAXIS.

For help, visit the VMWare web site.

Deploy the *.VHD Packages

You can deploy RealPresence CloudAXIS Suite as a virtual machine on Microsoft Hyper-Visor (Hyper-V) Server 2012 R2 using the VHD files included in the RealPresence CloudAXIS Suite software package.

To deploy RealPresence CloudAXIS Suite as a virtual machine:

1. Download the appropriate software package from the Polycom RealPresence CloudAXIS Suite Support site.
2. Save the **.vhd** file on the hard drive where Hyper-V Manager is installed.
3. Open Hyper-V Manager and click **Windows > Virtual Machine** to create a new virtual machine for RealPresence CloudAXIS Suite.

   The **New Virtual Machine** wizard displays.
4. Click **Specify Name and Location**, and enter a name and location for the virtual machine.
5. On the **Assign Memory** tab, enter **8192MB** as the **Startup memory**. The default is 512MB.
6. On the **Configure Network** tab, select an active virtual switch.
7. On the **Connect Virtual Hard Disk** tab, select **Use an existing virtual hard disk**, and locate the RealPresence CloudAXIS **.vhd** file.
8. View the Summary of the virtual machine, and click **Finish**.

   The new virtual machine displays in the Hyper V Manager.

Add a Legacy Network Adapter

Before you can start your virtual machine with RealPresence CloudAXIS deployed, you need remove the adapter you chose in the wizard and add a legacy network adapter.

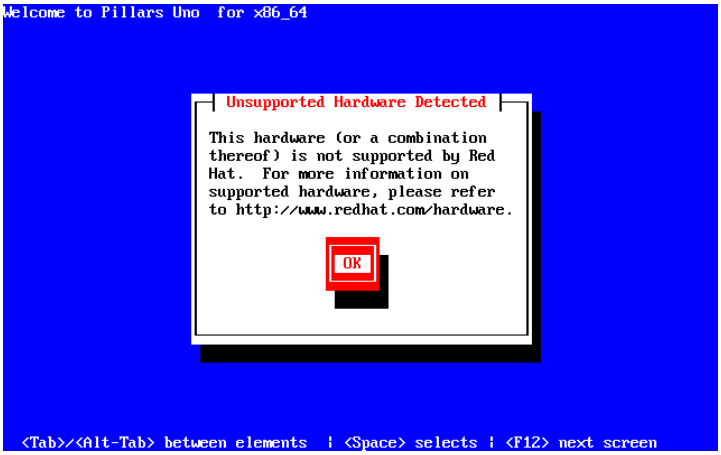
To add a legacy network adapter to your virtual machine:

1. Select your virtual machine and click **Settings**.
2. In the **Settings** window, select **Processor**, and change the value to **8**. By default, this is set to 1.
3. In the **Settings** window, click **Hardware > Legacy Network Adapter**.
4. Remove existing network adapters by selecting an adapter and click **Remove**.
5. Click **Add a Legacy Network Adapter**, and select the network adapter you want to add.

6 Click **Apply**.

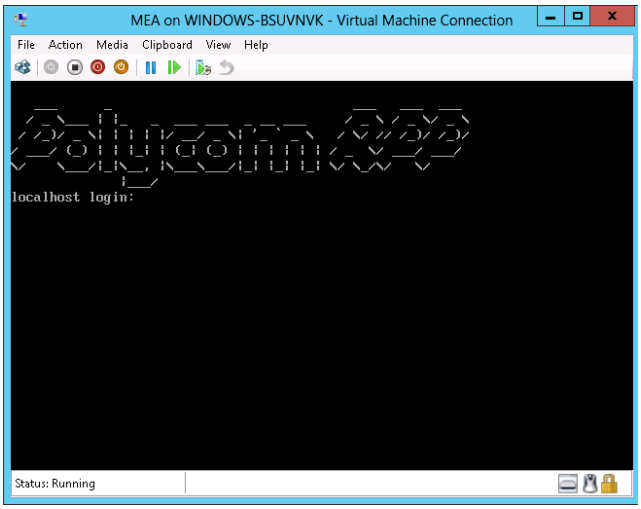
7 In the Hyper-V Manager, select your virtual machine and click **Start**.

A screen displays stating that unsupported hardware has been detected, as shown next.



8 Press the **Space** bar on your keyboard.

The installation continues, and the Hyper-V Manager restarts. After the restart, the login screen displays, as shown next.



Verify that Both Portals are Accessible

After you have deployed both portals and completed the basic network configuration, you can use a web browser to open the portals using the IP addresses and/or DNS names you assigned to them.

Admin Tip: For increased security, create at least one additional Super Admin account

To ensure secure administrator access to the RealPresence CloudAXIS Services Portal, after configuration is completed, we recommend that you create another account with Super Admin credentials to manage the RealPresence CloudAXIS Services Portal going forward. (See Create User Accounts for more information.) Login with the new Super Admin credentials, and then delete the default Super Admin account.

Open the RealPresence CloudAXIS Services Portal

Before you configure the RealPresence CloudAXIS Services Portal, you must obtain the FQDN assigned to the RealPresence CloudAXIS Services Portal and enter it into the address bar in your web browser.

To open the administrative and provisioning interface for the Services Portal:

1. Obtain the Services Portal's FQDN as referenced in your DNS server. Use the RealPresence CloudAXIS Services Portal FQDN you noted in the Setup Worksheet for the Server Settings.
2. Open a browser and enter the FQDN in the address bar to open the Services Portal login screen.
3. Log in to the Services Portal with Super Admin credentials.
4. For the first Services Portal login, type **admin** for the **Username** and **Polycom12#$**, and click **Login**.
5. When prompted, enter a new password for the default administrator account.

   For information on changing passwords, see Reset User Passwords.
6. Click **Agree** to accept the End User License Agreement (EULA) and proceed with the configuration.

You can now configure the RealPresence CloudAXIS Services Portal for use.

Open the RealPresence CloudAXIS Experience Portal

The RealPresence CloudAXIS Experience Portal provides a meeting interface that includes such features as content sharing, group chat, and privacy settings. All users who attend meetings require access to the RealPresence CloudAXIS Experience Portal.

To open the administrative and provisioning interface on the Experience Portal:

1. Obtain the Experience Portal's FQDN, as assigned through your DNS server.
2. In the address bar of your web browser, enter the Experience Portal FQDN with the port 9445 in the following format: **https://<*Server FQDN*>:9445**.
3. Log in to the Experience Portal administrator interface with Super Admin credentials.
4. For the first Experience Portal login, type **admin** for the **Username** and **Polycom12#$** for the **Password**, and click **Login**.

   A second login screen is displayed and prompts you to change the password.
5. Enter new values for **Username** and **Password**, and retype the new password as indicated.
6. Click **Save**.

You can now begin configuring the RealPresence CloudAXIS Experience Portal to be accessed by users to schedule and attend meetings.

Note: End user access to the RealPresence CloudAXIS Experience Portal

End users access the RealPresence CloudAXIS Experience Portal with a web browser, using the URL in the following format: **https://<*Server FQDN*>**. No additional port number is required for end user access.

Authorized users of your RealPresence CloudAXIS Suite can create meetings and add contacts in the RealPresence CloudAXIS Services Portal and set up conference interactions in the RealPresence CloudAXIS Experience Portal. The *Polycom RealPresence CloudAXIS Suite User Guide* shows users how to complete those tasks.

Set Up RealPresence CloudAXIS Suite for the First Time

After both Portals have been deployed, you can log in to the Administrator interface in each portal to start configuring the platform and conference settings for each. Because the Services Portal contains some of the configuration for both portals, configure it first.

Note: Log in with Super Admin credentials to complete all configuration steps

All configuration steps on both the RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal must be completed by a user with Super Admin credentials. Log in the first time using admin/admin as the username and password then enter an e-mail address for the Super Admin account and change the password. If you do not setup an e-mail for the account, you are not notified of future password changes.
For information on the account roles, see Account Roles.

Configure Network Settings

Because the RealPresence CloudAXIS Services Portal and Experience Portal both operate as web servers within a virtual server environment, you must configure both virtual web servers with IP addresses and DNS names, and those addresses and names must be included in the network settings within your virtual server environment.

Assign IP Addresses for Both Portals

When the portal instances boot up, they attempt to obtain IP addresses using DHCP. You can use the vSphere client to view the IP and MAC addresses that your DHCP server has allocated for each instance. Make note of the addresses allocated for both portals.

Polycom recommends that you assign permanent IP addresses to the Services Portal and RealPresence CloudAXIS Experience Portal instances, rather than allowing them to obtain IP addresses through DHCP.

Modify the configuration in your DHCP server to map the instance IP address to the corresponding MAC address. See the following instructions to assign an IP address using the vSphere console.

To assign an IP address using the vSphere console:

1. Connect to the vSphere console using an SSH client.
2. Log in using **caxis** as both your username and password to open the Portal console.

   A second login screen is displayed and prompts you to change the password if the default password is still in use.
3. Enter **show_network_info** to view the current network settings.
4. Enter **change_network_settings** to modify the current network settings.
5. Modify your DNS server settings to include DNS names for the RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal within your organization's domain.

See Secure Shell and Restricted Shell Commands for more information on configuring TCP/IP and DHCP settings.

Modify Settings in your DNS Server

We recommend that you modify your DNS server settings to assign a FQDN to each instance within your domain and associate it with the permanent IP address you have selected. Include separate DNS names and IP addresses for the Services Portal and the Experience Portal.

Set the Time Zone and NTP Server

First, you must set the time zone on the Network Time Protocol (NTP) server on both the RealPresence CloudAXIS Services Portal and Experience Portal.

To set the time zone and NTP server using the restricted shell:

1. Open a command line interface on either the Services Portal or the Experience Portal.
2. Type **caxis** for both your **Username** and **Password**.

   A second login screen is displayed and prompts you to change the password if the default password is still in use.
3. Select the time zone you want to use by using the command **change_timezone**.
4. Type **ntpdate** at the command line to synchronize your server with the NTP server.
5. Repeat the above steps on the other portal.

Verify the Time Settings

After configuring the time zone and NTP server, verify the time settings in the RealPresence CloudAXIS Services Portal interface.

To verify time settings:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > DATE TIME**.

3. Verify that the **NTP Server** and **Time Zone** settings match those that you set in the command line interface.
4. If the settings do not match, click **UPDATE** to synchronize the date and time.

After configuring the network settings on the RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal, the web services for both portals restart to update to the new network settings.

Manage Trust Certificates and Certificate Signing Requests

The RealPresence CloudAXIS Services Portal and Experience Portal require a secure connection from any connected browser. When a secure connection is established, the browser receives a trusted certificate verifying the identity of the Services Portal and Experience Portal.

Note: Upload separate certificates to each RealPresence server component

The certificates created from CSRs generated by the Services Portal authenticate the user connection only to the Services Portal. The certificates created from CSRs generated by the Experience Portal authenticate the user connection only to the Experience Portal. You need to generate separate CSRs for the Services Portal and the Experience Portal.

Generate Certificates and Certificate Signing Requests

You can generate an external certificate signing request (CSR) that includes both the RealPresence CloudAXIS Experience Portal and RealPresence CloudAXIS Services Portal FQDNs in the SAN field. This CSR can be signed by a third-party Certificate Authority and uploaded to the portals. Upload the private key and signed public key to both the RealPresence CloudAXIS Services Portal and the RealPresence CloudAXIS Experience Portal.

To generate certificates and CSRs, you must send the CSRs to a third-party Certificate Authority for a digital signature. From your certificate authority, obtain both a certificate for your server and intermediate and root certificates necessary for the certificate chain to have a complete path to the Certificate Authority's root certificate, with all certificates in Base 64 format. After you have obtained the certificates, upload them to your experience portal. For instructions on uploading certificates, see Upload Certificates or a Certificate Chain.

Note: Supported certificate hash types

The RealPresence CloudAXIS Experience Portal and RealPresence CloudAXIS Services Portal support the following certificate hash types: SHA1, SHA256, SHA384, SHA512, MD5, and HMAC. Certificates made with RSA Encryption are currently not supported.

The certificates created from CSRs generated by the RealPresence CloudAXIS Services Portal authenticate the user connection only to the Services Portal. You need to send an externally generated CSR to a Certificate Authority then upload the signed certificate and key to the components and Services Portal.

Note: File extensions on certificate requests and certificates

When you generate a certificate request to be sent to a trusted authority, save the file with a **.csr* extension. The file extension for a certificate is **.cer*.

A separate CSR must be externally generated for the RealPresence CloudAXIS Experience Portal and RealPresence components. The certificates created from CSRs generated by the RealPresence CloudAXIS Experience Portal authenticate the user connection only to the RealPresence CloudAXIS Experience Portal.

Caution: Overwrite warning

Before completing the following procedure, be sure that new certificates or CSRs are required before generating new certificates. Generating a new certificate or CSR overwrites the previous one. To check, see View Certificates.

To generate certificates and CSRs in the Services Portal and CSRs in the Experience Portal:

1. Log in to the Services Portal or Experience Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > CERTIFICATE**
3. On the **Generate CSR/Certificate** tab, enter values in the text fields as described in the following table:

Field	*Values/Description*
Operation Type	In the drop-down menu, choose one of the following: • **CSR** Generates a CSR to send to a third-party Certificate Authority for a digital signature. • **Certificate** Generates a self-signed certificate (not applicable for the Experience Portal).
Type	This is set to **WebServer** by default.
Organization	Enter the name of your organization.
Organizational Unit	Enter the name of your organization unit.
Country	Enter the two-letter ISO code for the country where your organization is located.
State	Enter the full name of the state where your organization is located.
Location	Enter the location of your organization.

4. Click **GENERATE**.
5. Restart the Services Portal Server and the tomcat6 and nginx servers.

To restart the tomcat6 and nginx servers:

1. Using an SSH client, open the Services Portal restricted shell using its assigned FQDN.
2. Log in as a privileged administrator using **caxis** for both your **username** and **password**.
3. Restart the web-related servers using the following commands:
   - `services tomcat6 restart`
   - `services nginx restart`

View Certificates

Super Admins can use the certificate list to confirm whether a certificate is needed and to delete obsolete certificates.

To view certificates in the Services Portal or Experience Portal:

1. Click **PLATFORM SETTINGS > CERTIFICATE > Certificate List**.

   A list of certificates display.
2. Click **View** to next to the certificate you want to view.

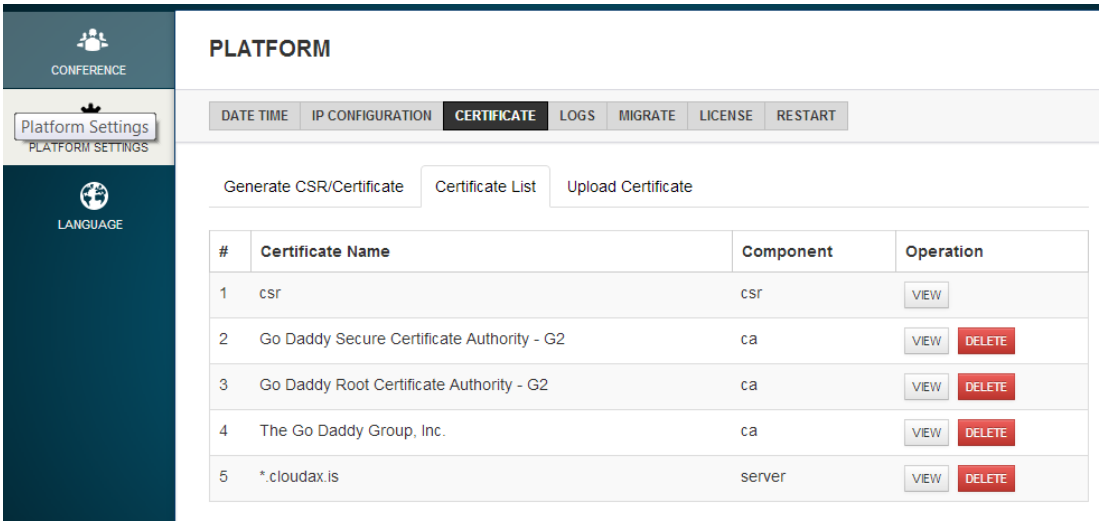
Copy a CSR

After you generate a CSR, you need to copy it from the RealPresence CloudAXIS Services Portal or Experience Portal and forward it to your preferred trusted certificate authority.

To copy a CSR:

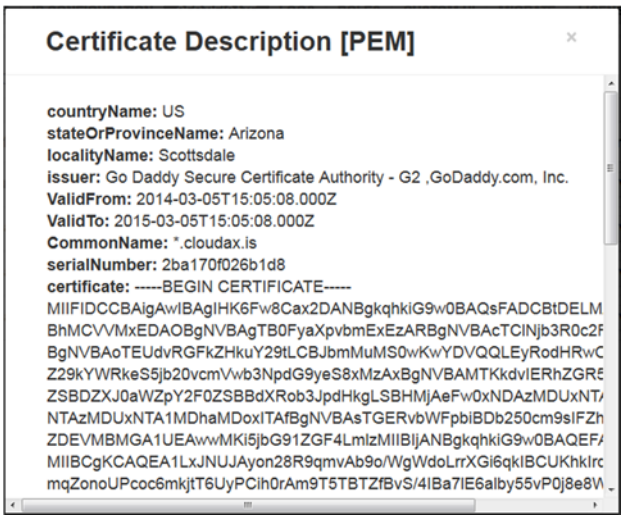
1. Log in to the Services Portal or Experience Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > CERTIFICATE > Certificate List**

   A list of certificates display.



3. Click **VIEW** next to the CSR you want to copy.

The **Certificate Description** displays, as shown next.



4 In the certificate screen, copy the entire hash from **----- BEGIN CERTIFICATE SIGNING REQUEST** to **----- END CERTIFICATE SIGNING REQUEST**.

5 Paste the text into a text editor.

6 Rename the file and save it with the file extension ***.cer** or ***.csr**.

7 Send the file to a third-party Certificate Authority for signing.

Delete Certificates

You can delete only WebApp-trust certificates.

Caution: Avoid deleting valid trust certificates

Deleting valid trust certificates can result in the issuance of invalid certificates and disrupt access to critical services in an organization.

To delete a certificate:

1 On the **Certificate List** tab, click **Delete** next to the certificate you want to download.

2 In the **Delete this certificate** dialog box, click **Delete**.

You can regenerate or upload web server certificates only as a Certificate Authority–signed certificate. To generate a WebApp certificate, see Generate Certificates and Certificate Signing Requests.

Upload Certificates or a Certificate Chain

Super Admins can upload certificates to the RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal. The Experience Portal certificates are separate from those uploaded to the Services Portal.

Upload a third-party, signed certificate to establish a secure communication with users and verify the identity information of RealPresence CloudAXIS Services Portal servers. Upload a trust certificate for servers that require secure communication, such as the Active Directory server, SMTP server, and RealPresence DMA system.

The following tables include the certificate types available for the Services Portal and Experience Portal.

RealPresence CloudAXIS Services Portal Certificate Types

Field Name	*Value/Description*
WebServer Private Key	A certificate generated by a trusted server.
WebServer Own	A private key certificate. It should match the Server Certificate
WebServer Trust	A certificate chain provided by the Certificate Authority.

RealPresence CloudAXIS Experience Portal Certificate Types

Field Name	*Value/Description*
Server Certificate	A certificate generated by a trusted server.
Server Key	A private key certificate. It should match the Server Certificate.
CA Certificate	A certificate chain provided by the Certificate Authority.

Note: Browser requirements for uploading certificates

Internet Explorer supports uploading certificates only in version 10 or higher. If you have Internet Explorer 8 or 9, download version 10 or use another browser, such as Chrome or Firefox, to upload certificates.

To upload a certificate:

1. Log in to the Services Portal or Experience Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > CERTIFICATE > Upload Certificate**.
3. From the **Type** drop-down menu, select a certificate type.
4. Click **Browse** or **Upload File** to navigate to and open the certificate or certificate chain you want to upload.
5. Click **UPLOAD**.
6. From an SSH command prompt, restart the nginx and Apache Tomcat servers using the following commands:
   - `services nginx restart`
   - `services tomcat6 restart`

7 Restart the Experience Portal services (see Restart the CloudAXIS Experience Portal Services or Server).

Configure Certificates for Reverse Proxy

To configure the RealPresence CloudAXIS Suite solution with Reverse Proxy, upload the signed public certificate of the RealPresence CloudAXIS Services Portal and the RealPresence CloudAXIS Experience Portal as trust certificates to the Reverse Proxy server.

RealPresence CloudAXIS Services Portal Server Settings

After you have deployed the RealPresence CloudAXIS Services Portal as described in the section Get Started, you can begin configuring the settings required for the Services Portal to run in your Polycom RealPresence environment.

You can complete the settings in any order.

Note: Save changes in each settings page before moving to the next menu

As you work through the settings and complete changes on a page, click **APPLY** to save changes before moving to another settings page. If you open a new page without saving changes, the settings revert to the previously saved changes.

Set Web Addresses for RealPresence CloudAXIS Portals

This section describes how to set up web addresses for the RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal servers. Each server has a specific purpose in the RealPresence CloudAXIS Suite environment:

- **Web Services Portal (WSP) Server** RealPresence CloudAXIS Services Portal where users create meetings.
- **Meeting Experience Application (MEA) Server** RealPresence CloudAXIS Experience Portal where all users join meetings.

To configure web addresses for the Services Portal and Experience Portal:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **SETTINGS > CORE SETTINGS > Server Settings**.
3. Enter configuration information for the two RealPresence CloudAXIS web servers, as shown next.

Setting	*Value/Definition*
MEA Server	The URL using the FQDN assigned to the IP address of the RealPresence CloudAXIS Experience Portal. See Open the RealPresence CloudAXIS Experience Portal.
WSP Server	The URL using the FQDN assigned to the IP address of the RealPresence CloudAXIS Services Portal. See Open the RealPresence CloudAXIS Services Portal.

4 Click **UPDATE** to apply the settings.

After you have confirmed that the Services Portal and Experience Portal are both available and accessible using a web browser, you can continue configuring the Services Portal.

Select a User Authentication Mode

The RealPresence CloudAXIS Services Portal handles authentication for users either using LDAP or Single Sign-On (SSO) authentication modes. The SSO mode also allows the use of LDAP as a back-up authentication.

Before you configure the settings for the mode of user authentication, you must select the method that will be used in the RealPresence CloudAXIS Services Portal, which handles authentication for both Services Portal and Experience Portal users.

Set Up LDAP Authentication

You can configure a connection to the LDAP server in your organization so that RealPresence CloudAXIS Suite users can be authenticated with their LDAP-enabled accounts. With LDAP enabled, administrators of the RealPresence CloudAXIS Services Portal can perform the following tasks:

- Import external user accounts from an enterprise
- Edit external user account default roles
- Set external user accounts as active or inactive

Note: RealPresence CloudAXIS Services Portal DNS server does not point to the Active Directory DNS Server

If the RealPresence CloudAXIS Services Portal DNS server does not point to the Active Directory DNS server, you need to add the SRV records of the Active Directory domain controller service in the Services Portal domain DNS server before updating the LDAP settings configuration. Create the SRV record in the Services Portal DNS server with the following details:

- **RR Type:** SRV
- **SRV record format:** _ldap._tcp.dc._msdcs.<*AD_DOMAIN_NAME*>.TTL class SRV priority weight port <*Canonical_hostname_of_Domain_Controller*>

For example:
If the Active Directory domain controller hosting the service for domain example.com is *ad_dc1.example.com*, then its SRV record would be as follows:
SRV RR: _ldap._tcp.dc._msdcs.example.com. 86400 IN SRV 0 100 389 ad_dc1.example.com

To configure a connection to an LDAP server:

1 Log in to the Services Portal with Super Admin credentials, and click **SETTINGS > CORE SETTINGS > AUTHENTICATION**.

2 Click **LDAP**.

3 Click **SETTINGS > CORE SETTINGS > LDAP**.

4 Enter information as outlined in the following table:

Setting	*Value or Description*
Forest Root Domain	Enter the forest root domain name for the company, for example *polycom.com* or m*icrosoft.com*.
Secure	Select to establish a secure connection to the LDAP server. This field is optional but recommended. Upload required certificates to the webserver-trust, and restart the Apache Tomcat server to establish a secure connection with the Active Directory server.
Port	Enter the numerical value of the port through which LDAP communicates. The standard port for LDAP is 389.
Username	Enter the user ID for the LDAP services account that has system access to the Active Directory.
Password	Enter the login password for the LDAP services account user ID.
Enable sub-domain search	Select if your organization has a root domain and sub-domain structure so that sub-domains can be searched. If this value is not selected, user searches occur only in the forest root domain. Enabling this option may slow search performance within Active Directory.
User default domain for authentication	If enabled, the default domain is used as an authentication prefix.
Default Domain	Enter the name of the default domain name where users are authenticated when a username is provided without a domain name.

5 Click **UPDATE**.

Set Up Single Sign-On Authentication

RealPresence CloudAXIS Suite applications can authenticate Windows and Mac OS X users internally using credentials entered when logging into the associated Active Directory domain. With Single Sign-On (SSO) enabled, users don’t need to re-enter Active Directory credentials on RealPresence CloudAXIS Suite portals if they are already logged into the domain.

Note: Android and iOS devices are not supported for SSO

The Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) version of SSO used in this release works only with Windows and Mac OS X devices logged into the Active Directory Domain. Android and iOS devices revert to LDAP when logged in to RealPresence CloudAXIS Suite, and users must enter credentials to log in to RealPresence CloudAXIS.

Before you configure SSO, you must first set up a user in your Active Directory Domain for the Services Portal. The tasks required for setting up Services Portal users in Active Directory are outlined in the section Appendix 1: Set Up Windows Active Directory for Single-Sign-On. Refer to the Microsoft support site for detailed instructions and for further information regarding SSO and the requirements for using it in your Active Directory domain.

Configure the RealPresence CloudAXIS Services Portal for Single Sign-On

After you have set up a user for the RealPresence CloudAXIS Services Portal in your organization's Active Directory domain, you can configure the SSO authentication method by updating the Service Principal Name and the corresponding keytab file as outlined below. If the SSO configuration is completed successfully, it attempts the SSO authentication while accessing the WSP service.

Note: Client devices and the Active Directory server must belong to the same enterprise domain

Client devices accessing the RealPresence CloudAXIS Services Portal and the Active Directory server must be members of the same enterprise domain for SSO to work correctly.

To configure the Services Portal for Single Sign-On:

1. Log in to the Services Portal with Super Admin credentials, and click **SETTINGS > CORE SETTINGS > AUTHENTICATION**.
2. Click **SSO (Single Sign On).**
3. Select the **Fallback to LDAP Authentication** check box if you want to users to be authenticated using LDAP in the event that SSO becomes unavailable.

   If you enable this option, also configure the LDAP settings (see Set Up LDAP Authentication).
4. In the **Service Principal Name** field, type the Service Principal Name that was created in Active Directory for the Services Portal domain user in this format: *HTTP/<wsp host name>.<domain name>@< DOMAIN NAME>*.

   For example, where the WSP host name is *wsp-sso* and the Active Directory domain is *cloudax.is*, the *servicePrincipalName* would be *HTTP/wsp-sso.cloudax.is@CLOUDAX.IS*

   Note: Use the syntax and case exactly as they display in the example.
5. In the **Kerberos Keytab File** field, click **Upload File** to select the keytab file that was created in your Windows Active Directory domain for the Services Portal user.
6. After the keytab file is successfully uploaded, click **UPDATE**.
7. Restart the Apache Tomcat server to apply the settings. From an SSH client command prompt, enter the following command:

   ```
   >> services tomcat6 restart
   ```

Configure Users' Internet Browsers to Use SSO

RealPresence CloudAXIS Services Portal requires a web browser that can perform Kerberos Authentication so that users can be properly authenticated and their browsers can be configured to recognize the trusted RealPresence CloudAXIS Services Portal site.

Browser Requirements for Kerberos Authentication

For RealPresence CloudAXIS Suite to successfully authenticate SSO using Kerberos, the following Internet Explorer requirements must be met:

- RealPresence CloudAXIS Suite must be running on a computer with Windows 2000, Windows XP Professional, or Windows 2003.
- The Active Directory domain controller must be Windows 2000 Server or later.
- RealPresence CloudAXIS Suite must be connected to the target Windows domain or a domain with a trust relationship with the targeted domain.

  Click **Start > Control Panel > System > Change Settings > Change**. Confirm that RealPresence CloudAXIS Suite is a member of the correct domain and not just a workgroup.
- The user who logged into RealPresence CloudAXIS Suite using Internet Explorer must be logged into the domain as well.

  Confirm that the Windows domain you are signed into on the computer is the target domain and not the local machine name.
- Integrated Windows Authentication must be enabled.

  In Internet Explorer, click **Tools > Internet Options > Advanced**. Select **Enable Integrated Windows Authentication**, click **Apply**, and restart Internet Explorer.
- Automatic logon must be enabled.

  In Internet Explorer, click **Tools > Internet Options > Security > Custom Level**. Make sure that **Automatic logon only in Intranet zone** for **User Authentication** is selected.
- The URL for the Services Portal must be listed in the Local Intranet zone.

  In Internet Explorer, click **Tools > Internet Options > Security > Local intranet** and confirm that the domain or host is listed.
- If your browser is configured to use a proxy server, the URLs for RealPresence CloudAXIS Suite portals must be added to the exceptions list. Integrated Windows Authentication does not work through proxies.
- The NTP must be functioning properly or some other method must be used to ensure that time synchronization between the URLs for RealPresence CloudAXIS Suite portals, the web server, and the domain controller is nominal. The time on the client, web server, and domain controller must all be exactly in sync.

If these requirements are not met, RealPresence CloudAXIS Suite may fallback to HTML form.

Configure Internet Explorer for SSO

For Internet Explorer users, you need to verify that Integrated Windows Authentication is enabled and add the Services Portal URL to the local intranet zone. Integrated Windows Authentication is usually set by default in Internet Explorer.

To verify Integrated Windows Authentication is enabled:

1. In Internet Explorer, click **Tools > Internet Options > Advanced**.
2. Select **Enable Integrated Windows Authentication**, click **Apply**, and restart Internet Explorer.

You also need to add the Services Portal to the local intranet zone. You can do this on individual computers or use Group Policy to update on the computers on the Active Directory.

To add the Services Portal to the local intranet zone on individual computers:

1. In Internet Explorer, click **Tools > Internet Options > Security > Local intranet > Sites** and click **Advanced**.
2. Enter the Services Portal URL in the **Add this website to the zone** field and click **Add**.
3. Click **Close > OK**.

To add the Services Porta to the local intranet zone using Group Policy:

1. Click **Start > Control Panel > Administrative Tools > Group Policy Management**.
2. Right-click **Group Policy Object** and click **Edit**.
3. Under **User Configuration**, click **Policies > Window Settings > Internet Explorer Maintenance**.
4. Click **Security** and double-click **Security Zones and Content Ratings**.
5. Under **Security Zones and Privacy**, select **Import the current security zones and privacy settings**.
6. Read the information about enhanced security configuration carefully. If the local intranet zone is considered a trusted zone without enhanced security configuration, click **Continue**. If the local intranet zone requires enhanced security, follow the directions on this screen and click **Cancel**.

   The Group Policy setting takes 90 minutes to refresh for all computers on the Active Directory.

Configure Other Browsers for SSO

Any settings you enable for Kerberos in Internet Explorer are reflected automatically in Google Chrome. Kerberos Authentication is not required for Safari on MAC OS computers.

For Mozilla Firefox, you do not need to enable Windows Integrated Authentication, but you can add the Services Portal site as a trusted site.

To add the Services Portal site as a trusted site for Firefox:

1. In Firefox, type **about:config** in the address bar.

   A warning dialog displays.
2. Click the confirmation dialog.
3. Type **network.negotiate-auth.trusted-uris** in the search bar.
4. Double-click **network.negotiate-auth.trusted-uris**, and add the URL for the Services Portal site.

   For example, *https://servicesportal.polycom.com*.

Enable E-mail Notifications for Users

The SMTP server enables the RealPresence CloudAXIS Services Portal to send e-mail notifications to users in the following situations:

- When their accounts are created
- When their account details are updated
- When they are invited to a meeting
- When a meeting they created or have been invited to is updated or canceled.

This section shows you the steps for configuring the connection to the SMTP server that forwards e-mails in your organization.

Note: Refer to documentation for your e-mail server for specific requirements

Mail servers may have specific requirements for configuring calendar invite e-mails. For example, Lotus Notes requires the following flag to be set to allow hosts to receive calendar e-mail invitations properly: CSAllowExternalIcalInviteToChair=1
For more information on Lotus Notes, refer to the following IBM TechNOTE: http://www-01.ibm.com/support/docview.wss?uid=swg21260593.
Refer to your e-mail documentation to review requirements for e-mail forwarding.

To enable e-mail notifications for the Services Portal:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **SETTINGS > CORE SETTINGS > SMTP**.
3. Enter values in the text boxes as outlined in the table shown next.

SMTP Settings	*Values/Definition*
Server	SMTP server FQDN or IP address
Secure	Select the check box to establish a secure SMTP-S/SSL connection. This is optional but recommended if the SMTP server supports secure connection.
Port	Enter the SMTP port number. Port 25 is commonly used for unsecure SMTP and 587 or 465 for SMTP-S.
Login ID	The account user ID for the SMTP service. This ID is not required for an unsecure connection.
Password	The password for the service account user ID login. This password is not required for an unsecure connection.
Sender Mail ID	The e-mail ID used to send notifications.

4. Click **UPDATE**.

Set Social Networking Policies

With social networking contacts enabled, users can send conference invitations to online contacts listed in their social networking accounts. Users can access social networking contacts directly in the Services Portal, but before Google+ users can access their social networking contacts, you must create an application that allows access to the contact list. See Appendix 2: Create Apps to Use with Social Media Contacts for more information. These applications share only the names and presence in the contact lists. Other personal information is kept private.

Enable Social Networking Contacts

After you have created an application for Google+, you must enable the social policy settings in the RealPresence CloudAXIS Services Portal.

To enable access to Google+ contacts for RealPresence CloudAXIS users:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **SETTINGS > SOCIAL POLICY**.
3. Select the check box for **Google+** to enable social policy options for that application.

   Selecting Google+ displays the configuration fields for that application.
4. Complete the fields for Google+ following the guidelines in the following table.

Social Policy Field	*Value/Definition*
App ID	Copy and paste the unique **App ID** that was generated when you created the app with Google+.
App Secret	Copy and paste the **App Secret** string that was provided to you when you created the app.
Auth Scope	Identifies which Google+ services the registered application has access to. The following values are used for Google+: • https://www.googleapis.com/auth/googletalk • https://www.googleapis.com/auth/userinfo.profile • https://www.googleapis.com/auth/userinfo.e-mail • https://www.googleapis.com/auth/calendar **Note**: Do not edit this field unless required or advised to.
Refresh Interval	Contains the interval at which the contacts and presence are synced from Google+.

5. Click **UPDATE**.

Disable Social Networking Contacts

You can disable social networking contacts at any time after they were enabled for RealPresence CloudAXIS users.

To disable access to social networking contacts in the Services Portal:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **SETTINGS > SOCIAL POLICY**.
3. Clear the check box for the app you want to disable, and click **UPDATE**.

Connect to a Polycom Access Point

Each RealPresence CloudAXIS environment must include at least one RealPresence Access Point, most commonly a RealPresence DMA server or RealPresence Access Director (RPAD) system. This section explains how to configure RealPresence CloudAXIS to work with your existing DMA and RPAD systems and other Polycom access points.

An *access point* is a network location that is routed directly or indirectly to the RealPresence DMA system. Clients or endpoints connect to conferences through an access point. The client or endpoint could be the RealPresence CloudAXIS Experience Portal, a separate soft client such as RealPresence Mobile, a hardware appliance such as Polycom® RealPresence® Group Series, or a telephone.

RealPresence DMA systems enable the RealPresence CloudAXIS Services Portal to launch online video conference meetings. RPADs are external links to the RealPresence DMA system that enable firewall traversal. Points of presence enable you to route either directly or indirectly to the RealPresence DMA system.

You can configure access points in the following ways:

- Direct connection to RealPresence DMA system
- External connection to access the RealPresence DMA system via H.323 video border proxy
- External route via a SIP Session Board Controller (SBC), including the RPAD system, or any third-party session boarder controller
- ISDN
- Audio dial-in via Public Switch Telephony Network (PSTN)
- External route from HTTPS Tunnel through RPAD

For example, an access point can be configured with an FQDN that points to the RPAD externally and to the RealPresence DMA system from within the network to enable the RealPresence CloudAXIS Services Portal to communicate with the RealPresence DMA system from either side of a firewall.

Each RealPresence CloudAXIS Suite environment must include at least one RealPresence DMA system or access point connection.

Note: At least one SIP access point is required in the RealPresence DMA system setup

The RealPresence CloudAXIS Services Portal must include at least one SIP access point.

Add a RealPresence DMA System and Access Points

You can add one RealPresence DMA system configuration with multiple access points to your RealPresence CloudAXIS environment. As you add access points, the system prioritizes them in the order in which they were added. You can change the pool order or conference template at any time.

To add a new RealPresence DMA system and access points to your RealPresence CloudAXIS configuration:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **SETTINGS > DMA CONFIG**.
3. Click **+ANOTHER DMA**.
4. Enter the appropriate data for **DMA CONFIGURATION** from your Setup Worksheet for the RealPresence DMA Server Access Point Configuration.

Setting	*Value*
Name	A nickname to assign to the RealPresence DMA system to distinguish it in the RealPresence CloudAXIS Services Portal configuration.
Host	The FQDN or IP address of a single node RealPresence DMA system or the virtual IP address or virtual FQDN of a RealPresence DMA system super node.
Port	The TCP port number used to communicate with the RealPresence DMA system. Port 8443 is standard.
VMR Prefix	The VMR prefix that corresponds to this RealPresence DMA system. The VMR prefix must match the prefix specified on the RealPresence DMA system. To set up this value, see the *Polycom RealPresence DMA 7000 System Operations Guide*.
Common SIP Username	(Optional) A username to authenticate SIP sessions for users who have authenticated with the RealPresence CloudAXIS Services Portal.
Common SIP Password	(Optional) A password for the Common SIP Username to authenticate SIP sessions for users who have authenticated with the RealPresence CloudAXIS Services Portal.
Default Admin	A username with system administrator privileges on the RealPresence DMA system.
Admin Password	The password for the Default Admin user.
Owner Domain	The domain of the user account assigned for creating meetings in the RealPresence DMA system. For local domains, enter **LOCAL**.
Owner Username	The username of the owner who creates meetings.
Generate VMR From Range	Select the check box to enter a range of numbers allowed for generating VMRs.

5 Click **+ ADD ACCESS POINT**.

6 Add new access points in the order that you want the Services Portal to use them and configure access points using the information shown in the following table.

For example, enter internal Access Points first. The system requires at least one SIP Access Point.

Field	*Enter values*
Location	A name for this access point that describes its geographic location or some other property that distinguishes it from other access points.
Transport	From the drop-down menu, select the protocol associated with the access point (SIP, TUNNEL, H323, ISDN, or PSTN). RealPresence CloudAXIS requires that you configure at least one SIP access point.
Dial string	The dial string that an endpoint should use to dial the access point. Your string should be appropriate for the specified access point transport type (for example, an ENUM for H.323).
Auth Mode	Select one of the following options: • **SHARED** Access points shared by all users. • **AUTH** Access points for those with enterprise credentials and who authenticate against the Services Portal. • **NOAUTH** For guest users who do not authenticate against the Services Portal. An AUTH mode access point requires a corresponding NoAUTH mode access point; conversely, a NoAUTH mode access point requires a corresponding AUTH mode access point.
Dial Prefix	(Optional) Specify a prefix to add to dialing information when dialing this access point. This prefix can be used by the access point to route the call or to distinguish between callers who are able to authenticate themselves from those that require unauthenticated guest access.

7 Click **+ADD ACCESS POINT** to enter another access point as needed.

8 When all required RealPresence DMA Configuration fields are completed, click **CONFIGURE**.

Admin Tip: Restart the Experience Portal after adding access points

Each time you add an access point in the RealPresence CloudAXIS Services Portal, you must restart the RealPresence CloudAXIS Experience Portal. See Restart the CloudAXIS Experience Portal Services or Server for information.

Change an Existing RealPresence DMA Connection

You can change settings in a RealPresence DMA connection that was set up in your RealPresence CloudAXIS environment. For details on the settings fields available for the connection, see the tables in Add a RealPresence DMA System and Access Points.

After you set up a RealPresence DMA connection, you can change the previously configured section and the following sections that are added after configuration:

- **MCU Pool Order** This feature is used by the users hosting or joining meetings using RealPresence CloudAXIS Suite.
- **Conference Template** This feature is applied to all scheduled and ad hoc meetings created on this RealPresence DMA system using RealPresence CloudAXIS Suite.

To change an existing RealPresence DMA connection:

1. Click › next to the RealPresence DMA host you want to configure.

   The **DMA Configuration** settings display.

2. Modify and verify the settings, and click **CONFIGURE.**

Set Conference Preferences

Conference preferences allow the Administrator to set and control how various meeting features display to users when they create and attend meetings.

To set conference preferences:

1. Login to the Services Portal with admin credentials.
2. Click **SETTINGS > CONFERENCE SETTINGS**.
3. Enter values in the text boxes as outlined in the following table.

Field	*Values/Description*
Passcode is mandatory	Select the check box to require an attendee passcode to be set for all meetings.
Chairperson Passcode Mandatory	Select the check box to require that meeting invites include a passcode for the meeting chairperson
AdHoc meeting duration	Enter the duration, in minutes, for Meet Now meetings. The default value is 120; the minimum duration is 15 minutes.
Buffer time before meeting starts	Specify how many minutes a meeting becomes active before its scheduled start time. The default buffer time is 10 minutes; the minimum is 1 minute.
Buffer time after meeting ends	Specify how long a meeting remains active after the scheduled end time. This setting has no default value; the minimum time is 0 minutes.

Field	*Values/Description*
Allow use of Personal VMR	Select the check box to allow the use of personal Virtual Meeting Rooms (VMR). When selected, the Use Personal VMR text and drop-down menu displays on the Schedule a Meeting screen.
Allow use of Join Bridge	Select this check box to enable the display and use Join Bridge button. When selected, the Join Bridge button is visible on the Web Portal home page. If not selected, the Join Bridge button is not displayed.
Expose Passcode	Select the check box to show the meeting passcode in the e-mail invite. If this option is not enabled, meeting hosts must notify invitees of the meeting passcode through some other means.
Enable Calendar Invite	Select the check box to send calendar invites when a meeting is scheduled, created or updated. If unchecked, an e-mail is sent with a calendar invite (*.ics) as an attachment.

4 Click **SET** to save the settings.

Add a Language Pack

Polycom provides a Language Pack that you can upload to the RealPresence CloudAXIS Services Portal to localize your RealPresence CloudAXIS Suite. You can upload only Polycom-authorized Language Packs into the Services Portal. Contact Polycom Support to request a new language pack.

To upload a language pack:

1 Click **SETTINGS > LANGUAGE**.

The Language Pack screen displays with the current version of the language pack uploaded to the Services Portal.

2 Click **Upload File**, select a Language Pack, and click **UPGRADE**.

You can click **View Supported Languages** on the Language Pack screen to view the languages available in the Language Pack.

Note: Revert the Services Portal to a previous Language Pack

You can return to an earlier version of a Language Pack by clicking **Revert To This Version**.

Customize E-mail Templates

You can customize the e-mail templates used to create and send meeting and user account management announcements. You can also view, download and edit, or replace any of the packaged e-mail templates. Only users with Super Admin privileges can edit e-mail templates.

Caution: Edit e-mail templates only if you understand HTML syntax

Edit e-mail templates only if you are familiar with HTML and understand how to edit HTML templates. If you intend to modify references or directives in the templates, you need to be familiar with Apache Velocity.
Before editing any template, review HTML Variables Used in E-mail Templates to understand how the WSP e-mail templates are structured.

To view an e-mail template:

1. Click **SETTINGS > E-MAIL**.
2. Click **View** next to the e-mail template you want to view.
3. From the **View Template** screen, click **CLOSE** to return to the **Customize e-mail templates** screen.

To download and customize an e-mail template:

1. Click **Download** next to the e-mail template you want to download.
2. Click **Open with** and choose a program, or click **Save**.
3. Edit the template using your preferred text or HTML editor.

Admin Tip: Template editing tools and tips

Edit templates using the Subline Text HTML Editor. See HTML Variables Used in E-mail Templates for information on how packaged RealPresence CloudAXIS Suite e-mail templates are structured.

To replace an existing e-mail template:

1. Click **Replace Template** next to the existing template you want to update.
2. Click **Select Template** and select the edited HTML file you want to upload.
3. Click **Preview and Upload** to view the template.
4. Click **Upload**.

Note: Template file size

Template file sizes are limited to 1MB per template. To keep the file size below 1MB, use URL links to add images to HTML templates, and ensure that users receiving the e-mail messages have access to the URL containing the images.

HTML Variables Used in E-mail Templates

Variables, methods, and conditional statements are referred to in Apache Tomcat as *references* and *directives*, which start with a $ or # tag (for example, `$Username`, `#if`, `#end`). The e-mail templates contain references and directives that are used to specify per-instance information that can be included in an e-mail generated from a template. These references and directives are dynamically replaced with information specific to the meeting or user management operation being reported.

Template files include both standard HTML instructions and references or directives that the RealPresence CloudAXIS Services Portal substitutes with instance-specific details when an individual e-mail is generated. References and directives can be added, moved, or removed, but only when they are defined as being valid for the type of e-mail message being used.

Commonly Used Directives

The following directives are used in e-mails concerning user and password management.

Directives for E-mail and Password Management

Directive	*Description*
`$FIRSTNAME`	First name of the user for which the account was created or the password was modified.
`$WSP_URL`	URL of the RealPresence CloudAXIS Services Portal on which the account was created or the password was modified.
`$USERNAME`	The username the user can use to log into the RealPresence CloudAXIS Services Portal.
`$PASSWORD`	The password the user can use to log into the RealPresence CloudAXIS Services Portal.

The directives in the following table are used in e-mails concerning meeting invitations and cancellations.

Directives for Meeting Invitations and Cancellations

Directive	*Description*
`$EVENT_STATUS_HEADING`	Set either to Invitation or Update, depending on whether the e-mail is being sent to announce a new scheduled meeting or one whose details have been modified, respectively.
`$EVENT_STATUS_BODY`	Set either to Created or Updated, depending on whether the e-mail is being sent to announce a new scheduled meeting or one whose details have been modified, respectively.
`$CREATED_BY_NAME`	The name of the user who has scheduled the meeting.

Directive	*Description*
$CREATED_BY_MAIL	The e-mail address of the user who has scheduled the meeting.
$EVENT_NAME	The name of the meeting as it was defined in the RealPresence CloudAXIS Services Portal.
$EVENT_TIME_GMT	The scheduled start time of the meeting expressed relative to Greenwich Mean Time.
$EVENT_DURATION	The scheduled duration of the meeting.
$EVENT_DESCRIPTION	The agenda of the meeting as defined in the RealPresence CloudAXIS Services Portal.
$VMR	The VMR number for the meeting.
$HTTPS	The secure web URL for joining the meeting.
$MEETING_PASSCODE	The passcode required to join the meeting.
$TOKEN	Encoded string which is hidden (by changing the text color to the background color) and which is read by HDX/GS to populate the meeting details in the calendar section of the respective device. It is present at the bottom of the page (just above the copyright). It is in the following format. DO NOT EDIT BELOW THIS LINE --=BEGIN POLYCOM VMR ENCODED TOKEN=--

Directives Associated with Endpoints

The following example construct in the template encloses an iterative loop so that all of the applicable access points (each `endpoint` in the script) are listed in the invitation:

```
#set( $geo = "null") #foreach( $endpoint in $endpoints ) #if($geo != $endpoint.getGeoZone()) #set( $geo = $endpoint.getGeoZone()) )#end #end
```

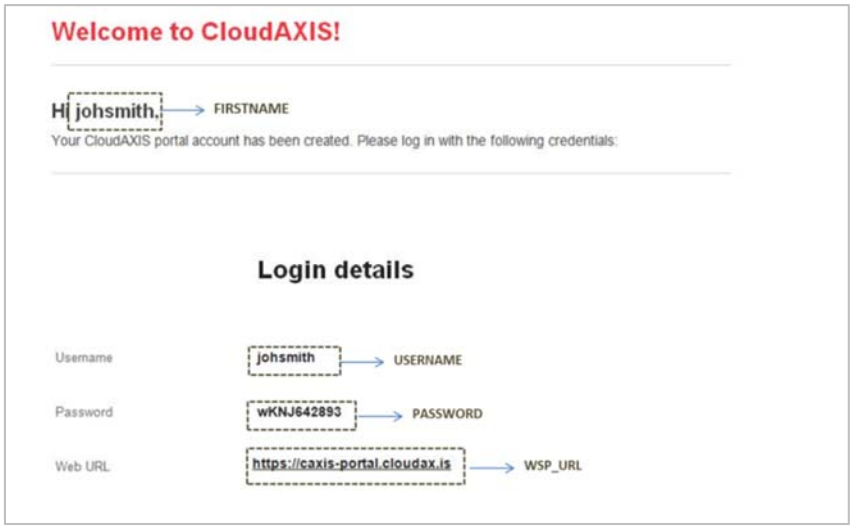
Use any of the following directives in the preceding loop to include appropriate endpoints in an invitation.

- **`$endpoint.getGeoZone()`** The location string associated with the current access point
- **`$endpoint.getTransport()`** The transport type (SIP, H.323, PSTN, and so on) associated with the current access point
- **`$endpoint.getUrl()`** The dial string associated with the current access point

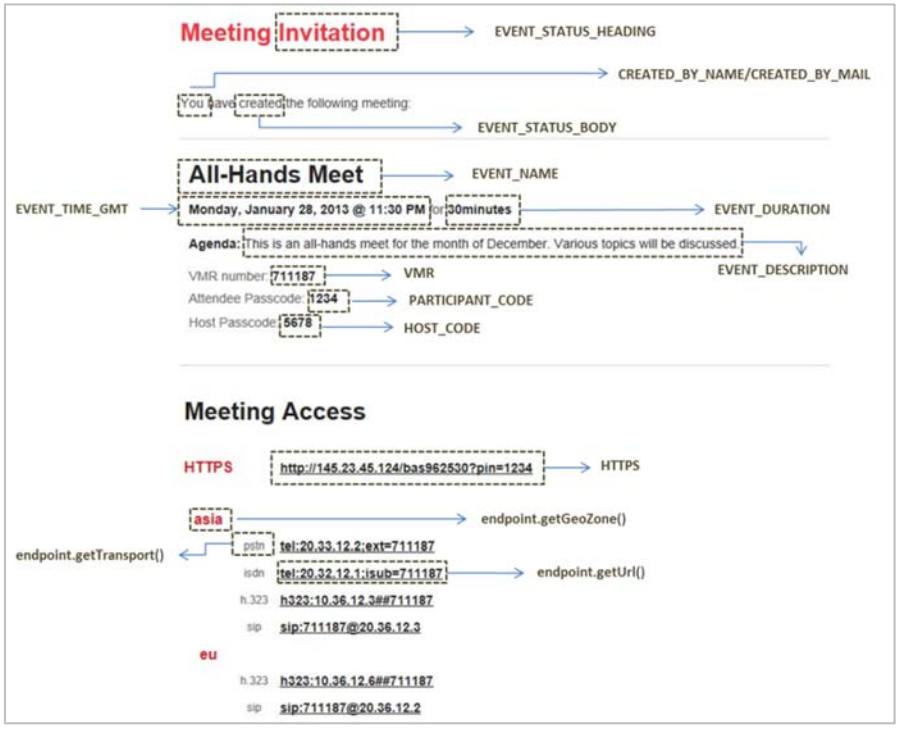
Sample Directives

The following are two sample template images that point to various references or directives.

$FIRSTNAME reference/directive



$EVENT_STATUS_HEADING reference/directive



Reset an E-mail Template

If you have customized an e-mail template but no longer want to keep the changes, you can reset it to the default template.

Any template that has been edited includes a **Reset** button among its options in the **Customize e-mail templates** page that allows you to revert to the original template.

To reset a template to the factory setting:

» On the **Customize e-mail templates** page, click **Reset** next to a template you have customized, as shown next.

Customize and White Label the User Interface

You can change the background, logo, application name, favorite icon, and other information on the RealPresence CloudAXIS Suite user interface to reflect a customized look and display your company's branding.

After you change any user interface settings in the Services Portal administrator interface, you must apply the changes in the Experience Portal administrator interface so that users can see the settings when they log in to the system.

Customize the User Interface

You can customize RealPresence CloudAXIS Suite user interface by changing the following user interface settings:

- The company logo that users see at the top of the browser window.
- The application title that displays. RealPresence® CloudAXIS™ displays by default.
- The favorite icon that displays when the application is launched in a new tab or window.

To change the general user interface settings in the Services Portal:

1. From the Services Portal administrator interface, click **SETTINGS > CUSTOM UI**.
2. On the **General** tab, click the **Logo** drop-down menu, and select **Custom** to display your company's logo or **Blank** if you do not want a logo to display.
3. If you selected **Custom**, click **Select** to browse for the new logo file, and click **Open**.

   Only logo files in .png, .gif, or.jpg format and less than 280 x 98 pixels are supported.
4. Click the **Application Title** drop-down list, and select **Custom**.
5. Type the name that your organization's users will see when they log in to schedule or attend a meeting. The maximum length for an application title is 75 characters.
6. Click the **Fav Icon** drop-down menu, and select **Custom**.
7. Click **Select** to browse to the file you want to use as an icon, and click **Open**.

   Only icon files in .png (recommended) or .ico format and less than 24 x 24 pixels are supported.
8. Click **UPDATE** to save the new UI settings.

After you customize the user interface in the Services Portal, you need to refresh the settings in the RealPresence CloudAXIS Experience Portal.

To refresh the user interface settings in the Experience Portal:

1. Open the Administrator interface on your Experience Portal.
2. Click **PLATFORM SETTINGS > CUSTOM UI**, and click **REFRESH**.

   A message at the top of the screen indicates whether the UI refresh was successful. You can log into the Experience Portal as a standard user to verify that the new UI is in place.

Change the Login Screen Display

You can change the background and choose to display both the logo and the application title on the screen that users see when they log in to a RealPresence CloudAXIS web portal to schedule or attend meetings.

To change the login screen display:

1. From the Services Portal administrator interface, click **SETTINGS > CUSTOM UI > Login Screen**.
2. Click **Display Logo on The Login Screen** and **Display Application Title on the Login Screen** check boxes.
3. To change the **Background**, select **Custom** from the drop-down menu.
4. Click **Select** to browse for a file, and click **Open**.

   The background file must be a .jpg no larger than 5 MB in size.
5. After you have uploaded a new background file, click **Preview** to see the Login Screen, and click **UPDATE** to save the changes.

Add a Notification Message for Users

You can add a message that displays for users on the Login screen, and you can schedule a time range for how long the message displays.

To display a notification message on the Login screen:

1. From the Services Portal administrator interface, click **SETTINGS > CUSTOM UI > Notification Message**.
2. Select the **Display Message** check box.
3. Enter a **Title** and **Message** in the text fields.
4. If you want to specify specific dates to display the message for users, click **Schedule this Message**.
5. Click to select the dates and times that you want to start and end the message.
6. Click **UPDATE**.

Add a Logout URL

You can choose to add a URL that redirects users when they log out of the system.

To add a logout URL:

1. From the Services Portal administrator interface, click **SETTINGS > CUSTOM UI > Footer / URLs**.
2. In the **Logout URL** section, select **Custom URL** from the drop-down list.
3. Paste or type the http address for the web page that you want to redirect users to.
4. Click **UPDATE**.

If SSO is enabled by the Super Admin and the custom logout URL is set, then if a user wants to log in as an admin or Super Admin after logging out of their user account, the user must use https://<WSPaddress>/login/#reln.

Add a Footer to the User Interface

You can choose to add a footer to display product information or provide a link to a help URL on the user interface.

To add a footer to the user interface:

1. From the Services Portal administrator interface, click **SETTINGS > CUSTOM UI >Footer / URLs**.
2. In the **End User Footer Settings** section, select the **Product Info** or **Help** check box.
3. If you selected **Help**, click the drop-down menu and select **Default URL** or **Custom URL**.
4. Paste or type the http address for the web page that you want to display to end users.
5. Click **UPDATE**.

Caution: Restoring settings to default

When you edit settings, you have the option to update or restore settings to default. When you choose to restore settings to default, the settings on the selected tab are restored to the settings that were in place when RealPresence CloudAXIS was deployed, not the last saved settings.

Refresh Custom User Interface Settings

After you customize the user interface settings in the Services Portal, you must refresh the settings in the Experience portal.

To refresh the custom user interface settings in the Experience Portal:

1. Log into the Experience Portal as a Super Admin.

2 Click **Platform Settings > Custom UI > Refresh**.

RealPresence CloudAXIS Services Portal Platform Settings

This section provides information on setting general platform settings for the RealPresence CloudAXIS Services Portal.

Note: Save changes in each settings page before moving to the next menu

As you work through the settings and complete changes on a page, click **APPLY** to save changes before moving to another settings page. If you open a new page without saving changes, the settings revert to the previously saved changes.

Set the Server Date and Time

The RealPresence CloudAXIS Services Portal uses a Network Time Protocol (NTP) Server for basic clock synchronization. You can set the date and time for the RealPresence CloudAXIS Services Portal.

In order for RealPresence CloudAXIS meetings to occur and for calls and recordings to work properly, both the RealPresence CloudAXIS Services Portal and the RealPresence CloudAXIS Experience Portal must reference the same time zone and NTP server.

You can confirm that the NTP date and time zone of your EXSi host matches the time on the Services Portal and Experience Portal. The default time for instances is taken from the EXSi. If that time is wrong, the Services Portal scheduler can go out of sync. The Services Portal time settings should also match those on the associated RealPresence DMA system.

Use the information you entered in the Setup Worksheet for the Date Time Configuration to complete this setting.

To set the date and time on the Services Portal:

1. Click **PLATFORM SETTINGS > DATE TIME**.
2. In the **NTP Server** text box, enter the IP address or FQDN of the NTP server being used to synchronize the time in your RealPresence CloudAXIS environment. This value must match the data supplied to the Experience Portal.
3. Select a **Time Zone** from the drop-down menu.
4. Click **UPDATE**.

View and Download Logs

When you select a log level, the RealPresence CloudAXIS Services Portal begins producing logs at the specified level of information. When you are ready to view log files, you can download the log files.

The following table lists the types of log levels available on the RealPresence CloudAXIS Services Portal.

Log Level Types

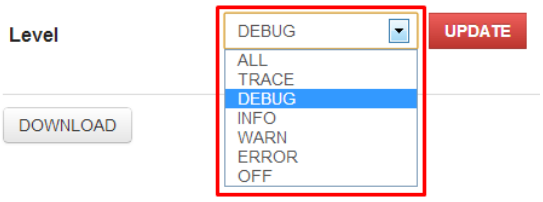
Log Level	*Description*
ALL	Turns on all logging.
DEBUG	Logs fine-grained information that is helpful for debugging.
TRACE	Logs more detail than a Debug log. These logs are also helpful for debugging.
INFO	Logs messages that highlight the progress of the application at a coarse-grained level.
WARN	Logs conditions that can be potentially harmful to the server environment.
ERROR	Logs errors that might allow the RealPresence CloudAXIS Services Portal to keep running.
OFF	Turns off logging.

Note: For day-to-day operations, set the log level to INFO

Polycom recommends setting logging to INFO or below. Set to more detailed levels when you're troubleshooting an issue, and return the setting to INFO or below for day-to-day operations.

To set the log level:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > LOGS**.
3. Click the **Level** drop-down menu and choose a logging level.



4. Click **UPDATE** to begin logging from the selected level.

To download the log files:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > LOGS**.
3. Click the **Level** drop-down menu and choose a logging level.
4. Click **Download**.

   The file downloads in a zip file.

Note: Log level hierarchy

When a log level is selected, all levels of logging beneath the selected level are included in the information. For example, if you choose INFO in step 2, the DEBUG and TRACE levels also display in your downloaded logs.

Update RealPresence CloudAXIS Services Portal Software

If you are currently running RealPresence CloudAXIS Suite, you can upgrade your RealPresence CloudAXIS Services Portal software and migrate the current configuration settings into the updated portal.

Before migrating the configuration settings, obtain the software for the new version you want to install, and deploy it on your VMWare host server.

To update RealPresence CloudAXIS Services Portal software:

1. Obtain the new Services Portal software *.OVA file from the Polycom Support Site.
2. Deploy the file using the instructions found in Deploy the *.OVA Packages.

Use the instructions in the following section to migrate the provisioning and state information from the existing portal running to the new portal.

Migrate Current Settings to the New RealPresence CloudAXIS Services Portal

When you update the RealPresence CloudAXIS Suite software, you can use the migrate process to export settings from the current system and import them into the new one.

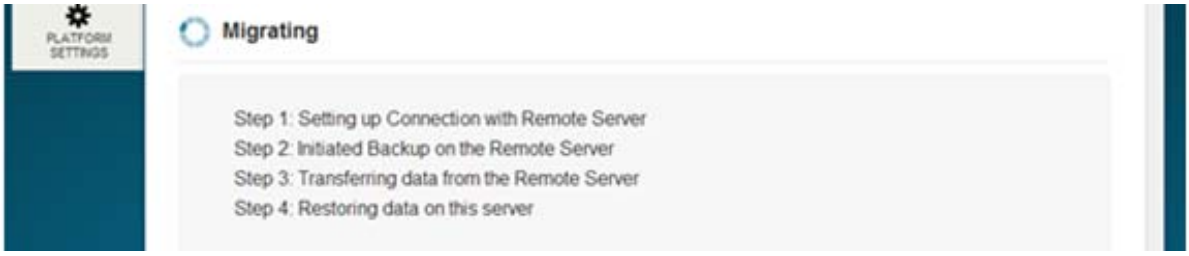
Before you begin the migrate process, verify that you have already loaded the correct certificates on the new RealPresence CloudAXIS Services Portal to which you want to migrate the settings. Deactivate the software licenses on old portals before you begin the process. See Upload Certificates or a Certificate Chain for information.

To migrate current Services Portal settings to a new Services Portal:

1. In the new Services Portal, click **PLATFORM SETTINGS > MIGRATE.**
2. Enter your credentials.
3. Read the disclaimer on the Platform Migration page and click **YES** when you are ready to begin the migration.
4. In the **Remote system details** screen, enter the **Hostname** (FQDN), **Admin Username**, and **Password** of the Services Portal from which you want to migrate the settings and database.
5. Click **MIGRATE**.

6 Wait for the user interface to indicate that the information from the old Services Portal was successfully imported. After the data has been imported, additional configuration runs in the background before the Services Portal reboots.

During these processes, the following screen displays.



7 After the Services Portal has restarted, log in to the new Services Portal with the admin credentials from the old Services Portal, and verify that the settings are correct.

Note: Verify the DNS records for the new RealPresence CloudAXIS Services Portal

After the data is successfully migrated, verify that the DNS records are updated to point to the new RealPresence CloudAXIS Services Portal. Alternatively, you can shut down the old Services Portal and set the new one to take its IP address.

Monitor the RealPresence CloudAXIS Environment

RealPresence CloudAXIS Suite uses the Simple Network Management Protocol (SNMP) application-layer protocol to monitor instances of Polycom RealPresence products that support SNMP monitoring.

If your RealPresence CloudAXIS Suite is running within a RealPresence Platform Director environment, you can monitor the Services Portal and Experience Portal through the RealPresence Platform Director interface.

SNMP Framework

The SNMP framework includes the following parts:

- **The SNMP manager** The system used to control and monitor the activities of network hosts using SNMP. A variety of network management applications are available for use with SNMP. It is important that you understand how your SNMP management system is configured to properly configure your Polycom system SNMP transport protocol requirements, SNMP version requirements, SNMP authentication requirements, and SNMP privacy requirements. For information on using SNMP management systems, see the appropriate documentation for your application.
- **The SNMP agent** The software component within the Polycom system that maintains the data for the system and reports this data, as needed, to managing systems. The agent and Management Information Base (MIB) reside on the same system.
- **The Management Information Base** A virtual information storage area for network management information, which consists of collections of managed network objects. You can configure the SNMP agent for a particular system MIB. The agent gathers data from the MIB, the repository for information about system parameters, and network data. Polycom systems include Polycom-specific MIBs with every system as well as third-party MIBs. Polycom MIBs are self-documenting, including information about the purpose of specific traps and inform notifications. Third-party MIBs accessible through the Polycom system can include both hardware and software system MIBs.

Polycom Use of SNMP

Polycom supports the following versions of SNMP:

- **SNMPv2c** Polycom implements SNMPv2c, a sub-version of SNMPv2, which uses a community-based form of security. The community of SNMP managers able to access the agent MIB is defined by an IP-based Access Control List and password.

  SNMPv2c does not encrypt communications between the management system and SNMP agents and is subject to packet sniffing of the clear text community string from the network traffic.
- **SNMPv3** Polycom implements SNMPv3, which provides secure access to systems with a combination of authenticating and encrypting packets over the network. The `contextEngineID` in SNMPv3 uniquely identifies each SNMP entity and is used to generate the key for authenticated messages. Polycom implements SNMPv3 communication with authentication and privacy.

- Authentication is used to ensure that traps are only read by the intended recipient. As messages are created, they are given a special key that is based on the `contextEngineID` of the entity. The key is shared with the intended recipient and used to receive the message.
- Privacy encrypts the SNMP message to ensure that it cannot be read by unauthorized users.
- Message integrity ensures that a packet has not been tampered with in transit.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. Notifications are sent, unsolicited and asynchronous, to the SNMP manager from the Polycom system. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to another system, or other significant events. They are generated as informs or trap requests.

Traps are messages alerting the SNMP manager to a system or network condition change. Inform requests (informs) are traps that include a request for a confirmation receipt from the SNMP manager. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. However, informs consume more system and network resources. Traps are discarded as soon as they are sent. An inform request is held in memory until a response is received or the request times out. Traps are sent only once, while informs may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and network resources.

SNMP notifications are only available in the RealPresence CloudAXIS Services Portal. The following table includes SNMP notifications and the severity and explanation for each.

SNMP Notifications

Notification	*Severity*	*Explanation*
ldapConnectionDown	Critical	The LDAP server is unreachable.
ldapConnectionUp	Informational	The LDAP server is no longer unreachable.
licenseExpired	Critical	The license has expired.
licenseServerDown	Informational	The license server is unreachable.
licenseServerOK	Informational	The license server is no longer unreachable.
dmaConnectionDown	Critical	DMA server <*name*> is unreachable.
dmaConnectionUp	Informational	DMA server <*name*> is no longer unreachable.
wspDown	Critical	The Services Portal server is down.
wspUp	Informational	The Services Portal server is up and running.
googleConnectionUp	Informational	The Google server is no longer unreachable.
googleConnectionDown	Critical	The Google server is unreachable.
smtpConnectionDown	Critical	The SMTP server is unreachable.

Notification	*Severity*	*Explanation*
smtpConnectionUp	Informational	The SMTP server is no longer unreachable.
meaConnectionUp	Informational	The Experience Portal server is no longer unreachable.
meaConnectionDown	Critical	The Experience Portal server is unreachable

Enable and Configure System Monitoring

You must enable and configure values in your system depending on the version of SNMP you want to use to monitor your RealPresence CloudAXIS Services Portal. You can use any SNMP client to monitor the health of your RealPresence CloudAXIS system.

You can implement SNMP over one of the following transport protocol versions:

- SNMPv2c is appropriate for standard communication models and uses community-based authentication.
- SNMPv3c is appropriate for high-security models and requires a security user for notifications.

Included in the SNMP configuration is a notification agent that notifies a selected user when significant system events occur.

To enable and configure SNMP on the Services Portal:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > SNMP**.
3. Select the **Enable SNMP Monitoring** check box

   The Configure SNMP fields display.
4. Click **Download MIB** to download a .zip file containing the management information base for the Services Portal.
5. Import the MIB definition into your SNMP manager to enhance its ability to monitor the target system.
6. Select the **SNMP version** from the drop-down menu.

   The configuration selections vary depending on which SNMP version you choose.
7. Complete the fields in the SNMP configuration section using the guidelines in the following table.

Field	*Value/Description*
Transport	The transport protocol to be used. RealPresence Platform Director supports only UDP at this time. UDP requires fewer network resources and is suited for repetitive, low-priority functions like alarm monitoring, although message delivery is not assured and does not always occur in the order in which messages are sent.
Port	The instance port on which the SNMP agent is running. The system is automatically configured to use port 161.
Community	Functions as a global password for accessing SNMP information on the system. An SNMP manager must be configured with the same community string in order to access this system's SNMP information. This field displays only when SNMPv2c is chosen. Per SNMP convention, the default community string is "public", but this can be changed to make the SNMP information more secure.
Location	The location setting enables you to supply the value to be returned for a standard MIB query that can help identify the geographical or logical location of the server.
Contact	This enables you to supply the value to be returned for a standard MIB query that can help identify the name or contact info of an administrator who is responsible for the server.
Security User	For SNMPv3 only. Specifies the security name required to access a monitored MIB object.
Encryption	For SNMPv3 only. Specifies the privacy protocol for the connection between the RealPresence Platform Director system and the SNMP agent. The RealPresence Access Director system implements communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB). Possible values for privacy protocol are: • No encryption • DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet.
Password (for encryption)	In the fields below the **Encryption** selection, enter the encryption password to be appended to the encryption key. Retype the encryption password in the **Confirm Password** field below.

Field	*Value/Description*
Authentication	Specifies the authentication protocol. These protocols are used to create unique fixed-sized message digests of a variable length message. Possible values for authentication protocol are: • MD5—Creates a digest of 128 bits (16 bytes). • SHA—Creates a digest of 160 bits (20 bytes). Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.
Password (for authentication)	For SNMPv3 only. In the field below the Authentication selection, enter the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest. Retype the encryption password in the **Confirm Password** field below.

8 Click **Add Agent** to configure a notification agent.

9 From the **SNMP Version** drop-down menu, select either version **v2c** or **v3**, and complete the fields using the guidelines outlined in the following table.

Field	*Value/Definition*
Transport	Select TCP or UDP.
Port	The default is 162. You can select a different port if 162 is in use.
Type	Select Trap or Inform. A trap is an unacknowledged notification while inform is acknowledged when received by the SNMP manager. This field should be set in accordance with the capabilities of the SNMP manager.
IP	The IP address or FQDN of an SNMP manager to which this system sends notifications.
Security User	v3 only. Select either **Create New** or **Use Existing**. If you choose to create a new user, you must select authentication and encryption protocols, along with passwords for each, as described in the previous **SNMP Monitoring Configuration** table. If you use an existing user, use the drop-down menu to select a user that is already in the system.

10 Click **ADD** to add the notification agent.

11 On the **Configure SNMP** screen, when you have finished editing the SNMP values, click **UPDATE**.

Caution: Resetting settings

When you edit settings, you have the option to update the system to save the new settings or reset the settings. When you choose to reset, the settings on the selected tab are restored to the settings that were in place when RealPresence CloudAXIS Suite was deployed.

User Management

Users in the RealPresence CloudAXIS environment are managed through the RealPresence CloudAXIS Services Portal, where accounts can be created locally through the Active Directory domain in which the Services Portal and Experience Portal are members.

To set up authentication with an LDAP server, or to set up Single Sign-On (SSO) for users in the RealPresence CloudAXIS environment, see Select a User Authentication Mode.

Account Roles

Except for the Super Admin account used to configure settings in the RealPresence CloudAXIS Experience Portal, user accounts for the RealPresence CloudAXIS environment are managed in the RealPresence CloudAXIS Services Portal. The application supports three account roles, each of which determines your account type and a different set of capabilities. Upon logging in to the RealPresence CloudAXIS Services Portal, each type of user sees a different menu reflecting the types of tasks each user is allowed to perform.

Caution: Set secure passwords for default required accounts

Change the passwords for default accounts as soon as possible. Failure to change them could allow any user to log in to the RealPresence CloudAXIS Services Portal with Super Administrator credentials. Make sure to enter an e-mail address for default accounts to receive notifications of any account changes.

The following table describes each role and the privileges and menu options visible to each role.

RealPresence CloudAXIS Account Roles

Role	*Primary Capabilities*	*Menu Options*
Super Admin	Manages the RealPresence CloudAXIS Services Portal settings and creates and edits other Super Admin, admin, and user accounts. The Super Admin cannot schedule meetings. A separate Super Admin account manages the Experience portal.	User Management Settings Platform Settings
Admin	Creates and manages admin accounts, user accounts, and online video conference meetings. This administrator cannot change server settings.	Schedule Calendar Address Book User Management
User	Creates, manages and attends online video conference meetings	Schedule Calendar Address Book

Note: Identifying your role

You can log in to the RealPresence CloudAXIS Services Portal and compare your menu with the preceding table to confirm the role you are signed in to the system with.

Manage User Accounts

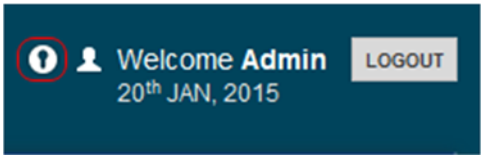
This section includes topics on managing user accounts.

Change System Administrator Password

Super Admins can change the System Administrator password at any time using the Administrator Settings menu.

To change the System Administrator password:

1. Log in to the Services Portal with Super Admin credentials.
2. Click in the upper right-hand corner of the Administrator user interface, as shown next.



3. Enter the **Current Password**, the **New Password**, and confirm the new password.
4. Click **CHANGE**.

Create User Accounts

Super Admins and admins can create RealPresence CloudAXIS accounts from the Active Directory or locally from the RealPresence CloudAXIS Services Portal. This section shows you how to add both active directory users and create local accounts.

The following table includes required default accounts that cannot be deleted. Make sure to change the password and add a valid e-mail address for each of the default accounts.

Required RealPresence CloudAXIS Suite Accounts

Field Name	*Value/Description*
admin	Use to access the RealPresence CloudAXIS Services Portal (Username/Password = admin/admin)
meaconf	Use for conference communication with the RealPresence CloudAXIS Experience Portal. (Username/Password = meaconf/meaconf)

Field Name	*Value/Description*
meaauth	Use for authentication communication with the RealPresence CloudAXIS Experience Portal. (Username/Password = meaauth/meaauth)
measys	Use for license communications with the RealPresence CloudAXIS Experience Portal. (Username/Password = measys/measys)

Add Active Directory Users

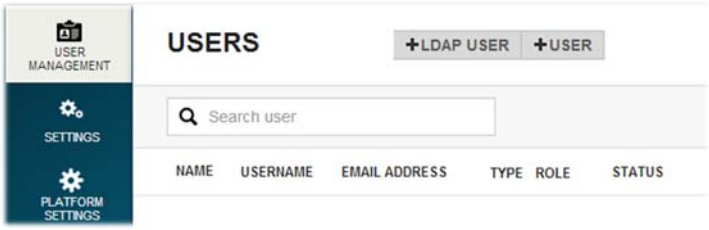
The LDAP server configuration grants access to the RealPresence CloudAXIS Services Portal for all the users in the Active Directory without requiring the administrator to create each RealPresence CloudAXIS Services Portal account. By default, the Services Portal assigns user roles to all the Active Directory accounts.

You can import Active Directory users into the Services Portal. These imported users are enabled automatically and remain enabled until their accounts are disabled. After the Services Portal is integrated with the Active Director server and that domain is allowed, all users of the domain can log into and use the Services Portal without further administrative action. Confirmation e-mails are not sent when an Active Directory user is imported.

Add a user from the Active Directory only if you need to change the default user role or block a user. To change the default user role, see Edit an Account Imported from the Active Directory.

To add Active Directory users to the CloudAXIS Services Portal:

1. Log in to the Services Portal with Admin or Super Admin credentials.
2. Select the **USER MANAGEMENT** tab to display the **USERS** screen, as shown.



3. Click **+ LDAP USER**.
4. In the **Import Active Directory Users** search field, enter the name of the user you want to add, and press **Enter**.
5. Select the check box next to each user you want to add.
6. Click **ADD**.

Note: Active Directory default user roles

Users added from the Active Directory are assigned the user role by default. To change the role type, see Edit User Accounts.

Add Local Users

In the RealPresence CloudAXIS Services Portal, Super Admin and admin users can add other local users. This section shows you how to create local accounts.

To add local users in the Services Portal:

1. Log in to the Services Portal with Admin or Super Admin credentials.
2. Select the **USER MANAGEMENT** tab.
3. On the **USERS** screen, click **+USER**.
4. Type the relevant user information in the text boxes provided.
5. Select a user type in the **User Role** drop-down menu. For more information on user types, see Account Roles.
6. Click **ADD**. An e-mail is sent to the newly created user containing his or her username, password, and URL.

You can edit and delete the accounts you create in the RealPresence CloudAXIS Services Portal. For more information, see the following sections.

Edit User Accounts

The RealPresence CloudAXIS Services Portal enables admins and Super Admins to edit accounts imported from the Active Directory or created locally. You can edit all fields for a local account, but you can access only two fields—role type and enable/lock—in an account imported from the Active Directory.

Edit an Account Imported from the Active Directory

You can edit only the role type and enable/lock options in accounts imported from the Active Directory. Only a Super Admin can change a role type to Super Admin.

To edit a user account imported from the Active Directory:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **USER MANAGEMENT**.
3. In the **USERS** screen, type the user's name in the search field and press **Enter** on your keyboard.
4. Click next to the account name.
5. From the **Edit User** screen, do one of the following:
   - Select a role type in the **User Role** drop-down menu.
   - Uncheck the **Enable User** check box to remove and disable the user's account.
6. Click **SAVE**.

Edit a Locally Created User Account

Super Admins can change all of the fields in a locally created account. Admins can change all of the fields in a locally created account except for the role in a Super Admin account. To determine your account type, see Account Roles.

To edit a local user account:

1. Log in to the Services Portal with Super Admin or Admin credentials.
2. Click **USER MANAGEMENT**.
3. Enter the user's name in the search field and press **Enter** on your keyboard, or find the account in the **NAME** column.
4. Click next to the account name.
5. Do one of the following:
   - To activate the user's account, check the **Enable User** check box
   - To remove and disable the user's account, clear the **Enable User** check box.
6. Click **SAVE**.

   An e-mail containing the username, password, and URL is automatically sent to the owner of the edited user account.

Delete User Accounts

Super Admins can delete other Super Admin, admin, and user accounts. Admins can delete only other admin and user accounts. To determine your account type, see Account Roles.

This section shows you how to delete a user account.

To delete a user account:

1. Log in to the Services Portal with Super Admin or Admin credentials.
2. Click **USER MANAGEMENT**.
3. Enter the user's name in the search field and press **Enter**.

   The user's name, username, e-mail address, type, role, and status are shown in the **USERS** search screen.
4. Click the ✖ next to the account name.
5. On the **Delete this User** screen, click **Delete** to remove the user.

Reset User Passwords

An Admin or a Super Admin can reset a user's password. This provides greater organizational security as it prevents former or unauthenticated members of your organization from being able to log in to the RealPresence CloudAXIS Services Portal.

Caution: Reset passwords only for users with valid e-mail addresses

Passwords should be reset only for accounts with valid e-mail addresses. Resetting a password for an account with an inactive e-mail address locks out the user.

To reset a password:

1. Log in to the Services Portal with Super Admin credentials.
2. Click **USER MANAGEMENT**.
3. Locate the user in the **NAME** column, or type the user's name from the **USERNAME** column into the search field and press **Enter** on your keypad.
4. Click ! next to the account.
5. In the **Change this user's password** dialog box, enter a new password in the **Password** field, and click **Change**.

   The RealPresence CloudAXIS Services Portal sends the user an e-mail containing the new password.

RealPresence CloudAXIS Experience Portal Conference Settings

After you have deployed the RealPresence CloudAXIS Experience Portal as described in Get Started, you can begin configuring the settings required for the Experience Portal to run in your Polycom RealPresence environment.

You can complete the settings in any order.

Note: Save changes in each settings page before moving to the next menu

As you work through the settings and complete changes on a page, click **APPLY** to save changes before moving to another settings page. If you open a new page without saving changes, the settings revert to the previously saved changes.

After you have finished configuring and customizing your RealPresence CloudAXIS Experience Portal, make sure to restart the portal services or server. See Restart the CloudAXIS Experience Portal Services or Server for instructions.

Set the Experience Portal Web Addresses

First, you must set the secure and non-secure, internal and external web addresses for the RealPresence CloudAXIS Experience Portal. External addresses allow users to access the portal, and internal addresses allow the Services Portal and Experience Portal to communicate with each other on the network.

Addresses in these settings are expressed in the form of a FQDN.

To configure web address settings for the Experience Portal:

1. Log in to the Experience Portal with Super Admin credentials.
2. Click **CONFERENCE > GENERAL SETTINGS**.
3. Click the **Enabled** check box.
4. Enter the **Web Addresses** settings as shown in the following table.

Field Name	*Value/Description*
Secure External Address	The HTTPS address that all users use to connect to the RealPresence CloudAXIS Experience Portal.
External Address (non-secure)	The HTTP address that all users use to connect to the RealPresence CloudAXIS Experience Portal. By default, it reroutes to the secure external address.

Field Name	*Value/Description*
Secure Internal Address	The address used for inter-agent communication within the server (not for users). This address includes the port number through which the portals connect to the Apache Tomcat server. By default, this is set to port 8443.
Internal Address (non-secure)	The non-secure address used for the inter-agent communication with the server (not for users). By default, it reroutes to the secure internal address.

5 Click **APPLY**.

Configure Conference Authentication Settings

The authentication rules in the RealPresence CloudAXIS Experience Portal determine which user accounts can authenticate against the RealPresence CloudAXIS Services Portal and access the RealPresence CloudAXIS Experience Portal either to host or attend meetings. You can also set rules that determine how users and guests are authenticated with the server.

Set Authentication Rules

Authentication rules comprise three fields: *Match, Property, and Realm*.

To set authentication rules for the RealPresence CloudAXIS Experience Portal:

1 Log in to the Experience Portal with Super Admin credentials.

2 Click **CONFERENCE > AUTHENTICATION**.

3 Complete the fields in the **Match**, **Property**, and **Realm** columns according the value descriptions in the following table.

Field Name	*Value/Description*
Match	Enter a regular expression that reflects the way you want the property to match for authentication. This value can reflect a host, domain host, or e-mail domain. For example, if you want to authenticate only users with a Polycom.com e-mail address, enter the regular expression **:+@*(polycom.com)$***
Property	This is the data type to which you want to apply the Match regular expression. Based on the user information entered, at least one rule is required for each property: • **SSOSource** The source of authentication for single sign-on users • **SSOUsername** The address of the Services Portal • **UserAddressDomain** A regular expression for the e-mail domain for SSO users • **Host** Match the provided regular expression against the host's URL to set the realm.

Field Name	*Value/Description*
Realm	The target authentication realm is the FQDN of the RealPresence CloudAXIS Services Portal server that you want to authenticate the rule against. UserAddress and SSOSource can point to the WSPAuth realm list using the *$#*, with *$1* referencing the first element in the list, and so on.

4 Click ⊕ to add additional rules and enter values for those rules.

5 Click ⇅ and drag the rules up or down based on the priority of the rules you entered.

Authentication matching starts at the first priority, moves down the list, and stops when the user's authentication method matches a listed rule.

6 Click **APPLY**.

Configure Services Portal Authentication

The RealPresence CloudAXIS Experience Portal must authenticate with the RealPresence CloudAXIS Services Portal to allow users to create and invite contacts to scheduled meetings. Configure settings in the RealPresence CloudAXIS Experience Portal to enable it to communicate with the RealPresence CloudAXIS Services Portal.

To configure authentication to the Services portal:

1 Log in to the Experience Portal with Super Admin credentials.

2 Select **CONFERENCE > AUTHENTICATION**.

3 Under **Agents**, expand the **Services Portal Authentication** settings.

4 Complete the rules for Services Portal Authentication according to the value descriptions in the following table:

Field Name	*Value/Description*
Target URL	The fully qualified domain name of the Services portal in your RealPresence CloudAXIS environment (HTTPS:// included).
Username	This field is populated with the name of the RealPresence CloudAXIS Services Portal authentication user. The default username is meaauth.
Password	Click **[!]** to enter login credentials for the meaauth user. The default password is meaauth.
Enforce Certificate Validation	Click the check box to enforce certificate validation of the certificate on the Services Portal. This is another level of SSL security that Polycom recommends using in a production environment, particularly if the RealPresence CloudAXIS Experience Portal is located near the internet in your network configuration.

Field Name	*Value/Description*
Realms	Enter the FQDN for your Services Portal without https://. Add the list of domains and user addresses that you configured in the match rules, separated by commas.
Allow domain users to bypass authentication and use guest login	Select the check box to allow authorized users authenticated in the Services Portal to join a meeting as a guest rather than an authorized user.

5 Click **APPLY**.

Configure Conference Rules and Settings

For RealPresence CloudAXIS to host meetings, you must configure routes, meeting settings, and external conference templates that determine the structure for meetings. A route confirms that the right agent is handling meeting requests.

An agent is set up on the RealPresence CloudAXIS Experience Portal for each type of meeting that can be conducted in a CloudAXIS meeting environment.

The VMR Conference Agent handles ad-hoc meeting requests held in a VMR with a URL and number to enter a meeting. These ad hoc meetings are handled by the local route *adhoc.caxis.local*.

The Services Portal Conference Agent handles scheduled meetings including the following types of meeting requests:

- Those scheduled in the Services Portal.
- Those entered using the Meet Now function in the Services Portal.

  These scheduled meetings are handled by the local route *scheduled.caxis.local*.

Set Conference Lobby Rules

Lobby rules define which of the two agents handles inbound meeting requests. You can set multiple lobby rules.

To set the Lobby Rules settings for the RealPresence CloudAXIS Experience Portal:

1 Log in to the Experience Portal with Super Admin credentials.

2 Click **CONFERENCE > CONFERENCE**.

3 Complete the fields in the **Match**, **Property**, and **Route** columns according the value descriptions in the table that follows.

Field Name	*Value*
Match	A regular expression for the matching VMRs that you want to access this lobby. For an ad hoc meeting, for example, those started with the Meet Now function, use a catch-all expression similar to *^[0-9]+* to allow any VMR number to work.
Property	What you want to apply the rule to; it can be either the lobby code or the host.
Route	The internal route for the lobby code match. Unless there is an explicit reason, this route *should not be modified*. The standard settings are: • *adhoc.cloudaxis.local* for ad-hoc meetings • *scheduled.cloudaxis.local* for scheduled meetings

4 Click ⊕ to add additional rules and enter values for those rules.

5 Click ⇅ and drag the rules up or down based on the priority of the rules you entered.

6 Click **APPLY**.

Configure the DMA Agent

All conference room requests get routed through the RealPresence DMA system that has been set up in your RealPresence system. The RealPresence DMA system also manages the meeting roster and controls recordings. The DMA Agent on the RealPresence CloudAXIS Experience Portal communicates with the RealPresence DMA system to manage and obtain meeting rosters and conference recordings.

To add a DMA Agent:

1 Log in to the Experience Portal (MEA) with Super Admin credentials.

2 Click **CONFERENCE > CONFERENCE**.

3 Under the **Agents** heading, expand the **DMA** menu to complete the settings for DMA agents according to the value descriptions in the following table.

Field Name	*Value/Description*
Target URL	The IP address or hostname of the DMA server, using this syntax: https://<*IP address or URL of the DMA*>:8443/api/rest
Username	The name of the default or configured admin user on the RealPresence DMA system. This user is the same as the admin entered for the DMA Configuration section of the Services Portal (see Add a RealPresence DMA System and Access Points).
Password	Click **[!]** to enter the password of the DMA admin user.
Enforce Certificate Validation	Select the check box to require that the RealPresence DMA system present a valid certificate for authentication to take place.

Field Name	*Value/Description*
Routes	This field is automatically populated with the information configured in the Lobby Rules settings. It should match the routes configured in those settings. Default routes are as follows: • *scheduled.cloudaxis.local* • *adhoc.cloudaxis.local*
Prefix	Enter the dialing prefix exactly as it displays on the DMA conference settings page. Enter “0” if no dialing prefix is used.

4 Click **Apply**.

Configure the VMR Agent and VMR Conference Settings

The following settings that provide information that routes users to VMRs where their meetings are scheduled.

To add a VMR agent on the Experience Portal:

1 Log in to the Experience Portal with Super Admin credentials.

2 Click **CONFERENCE > CONFERENCE**.

3 Under the **Agents** heading, expand the **VMR** menu to show the **Routes** dialog box.

Confirm that the setting reflects the default route to the VMR agent: *adhoc.cloudaxis.local*.

Next, configure the settings that determine the behavior of virtual meetings that meeting attendees join from the RealPresence CloudAXIS Experience Portal. Most of these settings are populated by default.

Configure VMR Settings

VMR settings determine how meetings occur in Virtual Meeting Rooms that users and endpoints can join to participate in a multi-party videoconference.

To configure Virtual Meeting Room (VMR) settings:

1 Log in to the Experience Portal with Super Admin credentials.

2 Click **CONFERENCE > CONFERENCE**.

3 Within the **VMR** menu, expand the **Settings** submenu.

Verify that the Routes field shows a route from the Lobby Rules that the VMR agent has access to, for example *adhoc.cloudaxis.local*.

4 Enter values in the **Settings** fields as outlined in the following table.

Field Name	*Value/Description*
Allow Anonymous Participants	Select the check box to allow participants who have not been authenticated against the Services Portal. If the check box is not selected, unauthenticated guest users are blocked from attending meetings.
Show End Meeting options	Provides attendees with the option to leave the meeting or end the meeting for all.
Require Display Name	Prompts anonymous attendees to enter a name before entering meetings.
Media Preferences	Default values are assigned in these settings. You can adjust them based on available bandwidth in your environment. We recommend that these settings match the settings in the RealPresence DMA system's conference template. Set the bandwidth allocated for each call by increasing or decreasing the default numbers for the following settings: • **Max SVC Call Rate** The initial call rate at which the client attempts to connect for an SVC call. • **Max AVC Call Rate** The initial call rate at which the client attempts to connect for an AVC call. • **Max AVC Tunnel Call Rate** The initial call rate at which the client attempts to connect for an AVC call in HTTP tunneled mode. Polycom recommends that this value be set lower than the value for non-tunneled calls.

5 Click **Apply**.

Configure the External Template for VMR Conferences

After configuring the VMR settings, you can configure the External Conference Template. These settings route RealPresence CloudAXIS plug-ins to their appropriate meeting rooms. The settings should match the access point settings configured in the RealPresence CloudAXIS Services Portal.

The External Conference Template determines how various users enter your RealPresence CloudAXIS environment through their allowed access points. At a minimum, access points should be set up for each type of user that can access your RealPresence CloudAXIS environment in the following ways:

- Users from outside your network firewall (external)
- Users from within your network firewall
- Users accessing through an HTTP tunnel, for far-end firewalls that do not allow outgoing SIP traffic

To configure the External Template for VMR Conferences:

1 Log in to the Experience Portal with Super Admin credentials.

2 Click **CONFERENCE > CONFERENCE**.

3 Within the **VMR** menu, expand the **External Conference Template** submenu.

4 Enter values in the fields in the **External Conference Template** for each access point in your RealPresence CloudAXIS environment, as outlined in the following table. These settings should match the settings for each access point set up in the RealPresence CloudAXIS Services Portal.

Field Name	*Value/Description*
Dial String	This value reflects the SIP dial string pointed to the FQDN of the RPAD system, as follows: *sip:{{LobbyCode|getvmr}}@[ExternalRPAD FQDN.domain.com]*
Location	Enter the city or office location of the POP server.
POP Address	Enter the FQDN or IP address of the access point being configured. This matches the value entered after the @ sign in the Dial String setting above.
Transport	Select an option from the drop-down menu to reflect the transport protocol used to connect calls in your RealPresence CloudAXIS environment. RealPresence CloudAXIS requires at least one SIP. • **sip** • **h323** • **ptsn** • **isdn** • **tunnel**
Authentication Mode	Select one of the following options from the drop-down menu: • **SHARED** Access points shared by all users • **AUTH** Access points for those with enterprise credentials and who authenticate against the Services Portal (WSP) • **NOAUTH** For guest users who do not authenticate against the Services Portal

5 Click ⊕ to add another access point.

6 For the **Conference ID** field, confirm that the ID matches the Conference ID set up in the **Lobby Rules** settings in the following format: *{{LobbyCode|getvmr}}*.

7 For the **Shared Credentials** field, enter the username and password configured on the RealPresence DMA system to allow external access. This is optional and required only if SIP Authentication is enabled on the RealPresence DMA system.

Next, configure the RealPresence CloudAXIS Services Portal Conference settings that determine how conferences authenticate and route through the RealPresence CloudAXIS Services Portal.

Configure the Services Portal Conference Agent and Conference Settings

The Services Portal Conference Agent communicates with the RealPresence CloudAXIS Services Portal to retrieve information about scheduled conference settings. The Services Portal agent then determines which options are available to users scheduling and attending meetings through the Services Portal.

To set up a Services Portal agent and conference settings:

1. Log in to the Experience Portal with Super Admin credentials.
2. Click **CONFERENCE > CONFERENCE**.
3. Expand the **Service Portal Conference** menu, and within that menu expand the **Settings** submenu.
4. Complete the settings as outlined in the following table.

Field Name	*Value/Description*
Target URL	Enter the complete URL of the Services Portal server.
Username	Enter the username of the Experience Portal conference user. The default is *meaconf*.
Password	If you have changed the password for the *meaconf* user, you must type the new user credentials in this field. The default is *meaconf*.
Enforce Certificate Validation	Select the check box to require that the Services Portal present a valid certificate for authentication to take place.
Routes	Make sure these routes match the information configured in the Lobby Rules settings. For example, *scheduled.cloudaxis.local* is populated as the route by default.
Allow Anonymous Participants	Select the check box to allow participants who have not been authenticated against the Services Portal (WSP). If the check box is not selected, unauthenticated guest users are blocked from attending meetings.
Require Display Name	Prompts anonymous attendees to enter a name before entering meetings.

Field Name	*Value/Description*
Media Preferences	Default values are assigned in these settings. You can adjust them based on available bandwidth in your environment. We recommend that these settings match the settings in the RealPresence DMA system's conference template. Set the bandwidth allocated for each call by increasing or decreasing the default numbers for the following settings: • **Max SVC Call Rate** The initial call rate at which the client attempts to connect for an SVC call. • **Max AVC Call Rate** The initial call rate at which the client attempts to connect for an AVC call. • **Max AVC Tunnel Call Rate** The initial call rate at which the client attempts to connect for an AVC call in HTTP tunneled mode. Polycom recommends that this value be set lower than the value for non-tunneled calls.

5 Click **Apply**.

Add Language Packs to the RealPresence CloudAXIS Experience Portal

You can configure the RealPresence CloudAXIS Experience Portal to display in one of several languages. The language settings in the RealPresence CloudAXIS Experience Portal should match those set in the RealPresence CloudAXIS Services Portal.

Localization capabilities include uploading a language pack.

Note: RealPresence CloudAXIS Experience Portal localization supported for the portal

RealPresence CloudAXIS Experience Portal localization is currently supported only for the user portal, not for the admin portal.

To upload a language pack:

1 Log in to the Experience Portal with Super Admin credentials.

2 Click **LANGUAGE**.

The current version of the language pack displays on the **Language** screen.

3 Click **Browse**, find the desired language pack, and click **UPGRADE**.

Manage User Roles

Users who attend meetings on the RealPresence CloudAXIS Experience Portal are assigned one of three roles: Chairperson, Participant, or Guest. The permissions they are allowed within a meeting they attend

are based on the role they have taken on or been assigned for that meeting. By default, the Chairperson, or the meeting creator, is given all available permissions in the meeting, a Participant can enter a meeting and share content, and a Guest can only enter the meeting. See View and Change User Permissions for information on changing permissions for participants or guests.

While a meeting is in progress, the Chairperson has the authority to change other users' roles for that meeting.

User Roles and Permissions

The following table outlines the user roles and default permissions in the RealPresence CloudAXIS Experience Portal.

Default User Roles and Permissions

Permission	*A user with this permission can …*	*Chairperson*	*Participant*	*Guest*
Enter meeting	Join the meeting.	✓	✓	✓
End meeting	End a meeting for all meeting users.	✓		N/A
Share content	Share content on his or her screen with other meeting attendees.	✓	✓	
Invite others	Invite additional users to attend the meeting.	✓		
Record meeting	Start and stop a recording of the meeting and all presented content.	✓		N/A
Promote users	Assign a new role to a user, including promoting a participant to a chairperson or a guest to a participant or chairperson. Assign, approve, or deny presentation rights in a meeting.	✓		N/A
Roster control	Mute or drop participants from the meeting roster.	✓		N/A

View and Change User Permissions

You can change the permissions for guests or participants or reset them to the defaults as shown in the preceding table. Chairperson permissions cannot be changed.

To view or change user permissions on the Experience Portal:

1. Log in to the Experience Portal with Super Admin credentials.
2. Click **Conference > Roles Management > Permissions**.
3. Select the check boxes to add or remove permissions for **Participant** or **Guest** user roles.

   A guest cannot be assigned the following roles (indicated by "N/A" in the preceding table):

- End meeting
- Record meeting
- Promote users
- Roster control

4 Click **APPLY**.

Roles Assignment

The administrator can set the roles assignments for meeting attendees, which determines how various users are initially assigned roles for the meetings they attend. Administrators can choose to assign attendees as chairpersons, participants, guests, or disabled. If disabled, users for that rule are assigned a different role that corresponds with how they were authenticated and how they joined the meeting.

The following table shows the default roles for meeting attendees based on how they have been defined for a given meeting and authenticated upon login.

Default Roles Assignments

Meeting Attendee	*Definition*	*Joins as …*
Owner	The owner of the VMR where the meeting is being hosted. This also applies to meetings hosted on personal VMRs where an owner has been assigned by the RealPresence DMA system.	Chairperson
Host	The person who scheduled the meeting, if applicable, and any other meeting attendee who has been made a host by the scheduler.	Chairperson
Invited users	Named users who were invited to the meeting by the host or by any other participant who has been given permission by the host to invite other users.	Participant
Users sharing owner domain	Users who are members of the Active Directory domain that the VMR owner is a member of.	Participant
Users sharing host domain	Users who are members of the Active Directory domain that the host user belongs to.	Participant
First user to join	The first user to join the meeting.	Disabled
Other authenticated users	Users who are authenticated with Active Directory credentials but are from a different domain than either of the host user and the VMR owner.	Participant
Unauthenticated users	Participants who have joined the meeting as a guest rather than an authenticated user.	Guest

View and Change Roles Assignments

An administrator can change how various users join meetings and are initially assigned roles for the meetings they attend.

To view or change user roles assignments on the Experience Portal:

1. Log in to the Experience Portal with Super Admin credentials.
2. Click **Conference > Roles Management > Roles Assignments**.
3. Click the drop-down menu to select a user type for the meeting attendee types listed.
4. Click **APPLY**.

RealPresence CloudAXIS Experience Portal Platform Settings

Platform Settings enable the RealPresence CloudAXIS Experience Portal to communicate with the RealPresence CloudAXIS Services Portal and other components in the RealPresence CloudAXIS environment. They also enable users to host and attend meetings through the RealPresence CloudAXIS Experience Portal.

RealPresence CloudAXIS Experience Portal settings that you configure are saved in the settings.json file, which you can export and save as a backup or import to another RealPresence CloudAXIS Experience Portal server.

Note: Save changes in each settings page before moving to the next menu

As you work through the settings and complete changes on a page, click **APPLY** to save changes before moving to another settings page. If you open a new page without saving changes, the settings revert to the previously saved changes.

Set the Server Date and Time

The server date and time must be in sync with the date and time on the Services Portal. To ensure that dates and times remain synchronized among the various RealPresence components, a Network Time Protocol (NTP) is used.

To set the server date and time:

1. Log in to the Experience Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > DATE TIME**.
3. Enter the address of the **NTP Server**.
4. Select a **Time Zone** from the drop-down menu.

   After the NTP Server and Time Zone have been set, the Date and Time dialog is updated automatically.
5. Click **UPDATE**.

Assign an IP Address to the Server

You can use DHCP to obtain a server IP address, or you can set a static IP address for the RealPresence CloudAXIS Experience Portal. The default configuration is set to use DHCP to obtain an initial address. However, Polycom recommends setting a static IP address for the RealPresence CloudAXIS Experience Portal server to use after the initial configuration.

To assign an IP address to the RealPresence CloudAXIS Experience Portal:

1. Click **PLATFORM SETTINGS > IP CONFIGURATION**.
2. Do one of the following:
   - Select the **Obtain an IP address automatically** check box if you want the Experience Portal server to obtain an IP address automatically using DHCP.
   - Clear the **Obtain an IP address automatically** check box if you want to assign a static IP address to the Experience Portal server and complete the fields for the IP address and DNS server settings that you have assigned to the server.
3. Click **UPDATE**.

Manage RealPresence CloudAXIS Experience Portal Log Files

The RealPresence CloudAXIS Experience Portal logs system transactions, errors, and events to help you monitor events and troubleshoot problems. The number and type of transactions that are logged in the system is based on the log level selected in the Log Settings. Log levels available in the RealPresence CloudAXIS Experience Portal include ERROR, INFO, and DEBUG. The more detail in a log, the more disk space required to store it, and the more system resources required to create it.

Set a level for logging based on what you want to accomplish. For instance, to help you troubleshoot a specific problem, you can set the log level to DEBUG to see a high level of detail in the logs and discover the source of the system problem.

You can also set a disk usage threshold to specify the maximum amount of available disk space that can be used to store log files.

Set the Log Level

The portal produces logs at the level you have specified in the Log Settings. The level of detail is greatest in DEBUG mode and least in ERROR mode. The system default is INFO.

Caution: Do not use DEBUG for day-to-day operations

Because debug logging captures every event, error, and transaction that passes through the system, debug logs produce a high amount of detail and require large amounts of disk space for storage. While these highly detailed logs are useful for troubleshooting a specific problem, we do not recommend DEBUG mode for day-to-day operations. Use ERROR or INFO for day-to-day operations.

To set the log level on the Experience Portal:

1. Log in to the Experience Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > LOGS**.
3. Click the **Level** drop-down menu and select **ERROR**, **INFO**, or **DEBUG** to set the level of detail you want to include in your logs.

4 In the **Disk Usage Threshold (DUT)** text field, set a threshold percentage that represents the maximum amount of available disk space that can be used to store log files.

   When the log storage reaches the set threshold level, the system automatically begins deleting stored logs, with the oldest logs deleted first.

5 Click **UPDATE** for the system to begin producing logs at the level you have selected.

Download and View Log Files

After the RealPresence CloudAXIS Experience Portal has logged information to help you troubleshoot problems, you can download copies of the log files that a system administrator or a Polycom Support representative can view.

To download log files:

1 Log in to the Experience Portal with Super Admin credentials.

2 Click **PLATFORM SETTINGS > LOGS**.

3 Click the **Level** drop-down menu and select **ERROR**, **INFO**, or **DEBUG** to set the level of detail you want to include in your logs.

4 In the **Select the Logs From** date fields, click to select a date range for the logs you want to view.

   Wait some time to let the system run long enough to generate enough log information to help you solve any issues that may be occurring.

5 Click **DOWNLOAD** to download a tar.gz file containing a set of system logs to your browser.

6 Open the individual log files within the tar.gz file.

Clear Log Files

You can remove all existing logs from the system.

To clear the log history in the RealPresence CloudAXIS Experience Portal:

1 Log in to the Experience Portal with Super Admin credentials.

2 Click **PLATFORM SETTINGS > LOGS**.

3 Click **CLEAR LOGS** to clear all of the existing logs from the Experience Portal.

Update RealPresence CloudAXIS Experience Portal Software

You can update your RealPresence CloudAXIS Experience Portal software when new software is available.

To deploy an updated version of RealPresence CloudAXIS Experience Portal software:

1 Obtain the new RealPresence CloudAXIS Experience Portal software *.OVA file

2 Deploy the *.OVA file using the instructions in Deploy the *.OVA Packages.

The following sections include information on migrating the provisioning and state information from the existing server to the new RealPresence CloudAXIS Experience Portal with the latest software version.

Export Current RealPresence CloudAXIS Experience Portal Settings

Configuration settings are saved in the RealPresence CloudAXIS Experience Portal settings.json file. This file can be exported from the current RealPresence CloudAXIS Experience Portal server and imported into a new RealPresence CloudAXIS Experience Portal server or saved as a backup. The file is downloaded locally and saved to the Downloads directory specified in your browser settings.

To export the RealPresence CloudAXIS Experience Portal configuration file:

1 Click to **PLATFORM SETTINGS > MIGRATE**.

2 When prompted, enter Super Admin credentials.

3 Click **EXPORT** and **Save File**.

The settings.json file is saved to your Downloads folder.

Import Settings to a New RealPresence CloudAXIS Experience Portal

The settings.json file contains all of the configuration settings for the RealPresence CloudAXIS Experience Portal. You can import a settings.json file from a previous RealPresence CloudAXIS Experience Portal to a newly deployed RealPresence CloudAXIS Experience Portal server.

Note: Restart the server to apply new configuration settings

After the configuration is imported, restart the server to apply the configuration. This deactivates the license if two instances of the RealPresence CloudAXIS Experience Portal are registered to the same RealPresence CloudAXIS Services Portal server. See Restart the CloudAXIS Experience Portal Services or Server for more information.

To import the Experience Portal settings:

1 Log in to the new Experience Portal with Super Admin credentials.

2 Click **PLATFORM SETTINGS > MIGRATE**.

3 When prompted, enter valid Super Admin credentials.

4 In the **Import Configuration** dialog, click **Browse**, find the **settings.json** file you want to import, and click **OPEN**.

5 Click **IMPORT** to upload the new settings.

6 Click **PLATFORM SETTINGS > RESTART > RESTART SERVICES** to apply the changes and restart the RealPresence CloudAXIS Experience Portal and the Administrator user interface.

Restart the CloudAXIS Experience Portal Services or Server

Changing settings in the RealPresence CloudAXIS Experience Portal often requires that you either restart the web services on the server or reboot the server.

Restart the RealPresence CloudAXIS Experience Portal Services

Restarting the services keeps the web server running while logging out all current users and ending all current calls.

To restart all of the services related to the Experience Portal:

1. Click **PLATFORM SETTINGS > RESTART** to open the **Restart** screen.
2. Click **RESTART SERVICES**, and in the confirmation window, click **OK**.

   The services are stopped and restarted. All users are logged out, and all calls are ended.
3. Open the Experience Portal URL, with **:9445** at the end of the URL, in a web browser to reconnect to the server as an administrator.

   For example, type https://<*experienceportal.domain.com*>:9445.

To Reboot the Server

Rebooting the server shuts down and restarts the entire RealPresence CloudAXIS Experience Portal virtual server.

To reboot the RealPresence CloudAXIS Experience Portal server:

1. Click **PLATFORM SETTINGS > RESTART** to open the Restart screen.
2. Click **REBOOT SERVER**. Then, in the confirmation window, click **OK**.

   The virtual server are stopped and restarted. All users are logged out, and all calls are ended.
3. Open the Experience Portal URL, with **:9445** at the end of the URL, in a web browser to reconnect to the server as an administrator.

   For example, type *https://<experienceportal.domain.com>:9445.*

Activate RealPresence CloudAXIS Suite Licenses

How you manage licenses in RealPresence CloudAXIS Suite depends upon whether you are operating your RealPresence CloudAXIS system in stand-alone mode or within a RealPresence Platform Director solution. In either process, you can use online mode if your RealPresence CloudAXIS Services Portal has a connection to the internet or offline mode if your RealPresence CloudAXIS Services Portal does not have a connection to the internet.

Use one of the following licensing procedures to license your RealPresence CloudAXIS Services Portal and RealPresence CloudAXIS Experience Portal.

Activate RealPresence CloudAXIS Suite Licenses within Platform Director

When you deploy a RealPresence CloudAXIS system within a RealPresence Platform Director solution, you must manage licensing through Platform Director for both the RealPresence CloudAXIS Services Portal and the RealPresence CloudAXIS Experience Portal.

Set Up Licensing on the RealPresence CloudAXIS Services Portal

First, you need to create a new instance of the RealPresence CloudAXIS Services Portal within the RealPresence Platform Director system. When you set up the RealPresence CloudAXIS Services Portal within a RealPresence Platform Director system, the RealPresence CloudAXIS Services Portal automatically connects to the RealPresence Platform Director licensing server and port.

See the *Polycom RealPresence Platform Director Administrator Guide* for further information about licensing RealPresence CloudAXIS Suite within that platform.

Note: Licensing for existing RealPresence CloudAXIS Services Portal instances

If you add an existing instance of a supported version of the RealPresence CloudAXIS Services Portal into a RealPresence Platform Director system, Platform Director automatically begins managing licensing for that instance. You must continue allocating licenses through RealPresence Platform Director as long as the RealPresence CloudAXIS Services Portal remains an active instance within that system.

To set up licensing for the RealPresence CloudAXIS Services Portal within RealPresence Platform Director:

1. Set up and configure a new Services Portal instance per the instructions in the *Polycom RealPresence Platform Director Administrator Guide* for creating a new software instance.
2. Change the administrator password in the Services Portal.

3 Navigate to the Services Portal settings in Platform Director, and change the password for this Services Portal Instance.

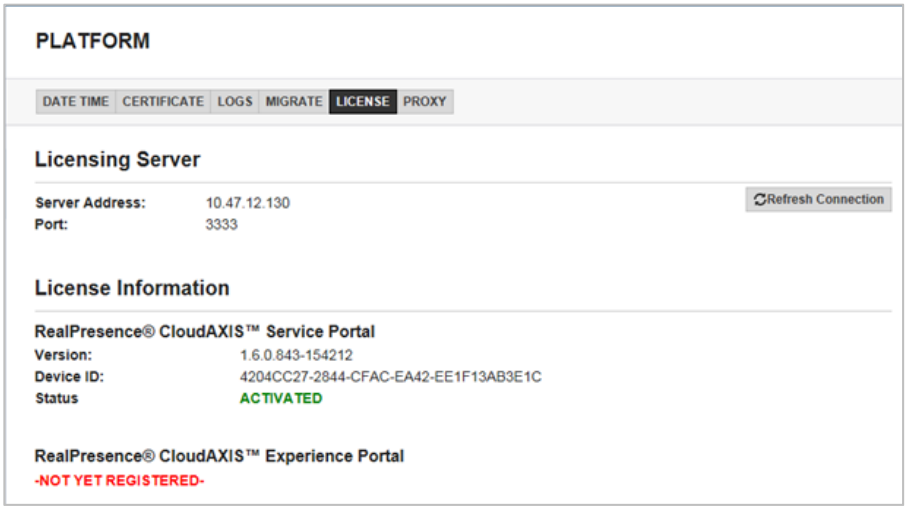
Passwords must match in both places for the RealPresence Platform Director to properly manage licensing for RealPresence CloudAXIS instances.

4 Log in to the administrator interface for the new the Services Portal using its FQDN and change the administrator password, when prompted.

5 From the Services Portal administrator interface, click **PLATFORM SETTINGS > LICENSE**.

6 Verify the following license settings, as shown next:

- The IP address for the **Licensing Server** is the IP address for the RealPresence Platform Director instance that manages this Services Portal.
- The Services Portal **License Information** reflects an activated license.
- The Experience Portal license is listed as not yet registered.



7 If the Server Address is incorrect, or the Services Portal does not show **ACTIVATED** as the status, click **Refresh Connection**.

8 Continue to the next section for instructions on setting up the license for the RealPresence CloudAXIS Experience Portal.

Note: RealPresence CloudAXIS Services Portal system password

The system administrator password set up in the RealPresence CloudAXIS Services Portal must be the same as the one you set up for it in the initial configuration you completed through RealPresence Platform Director when setting up the instance. If you set up a different password for the system when you set up the new RealPresence CloudAXIS Services Portal instance, you must change the password for that user in the RealPresence CloudAXIS Services Portal.

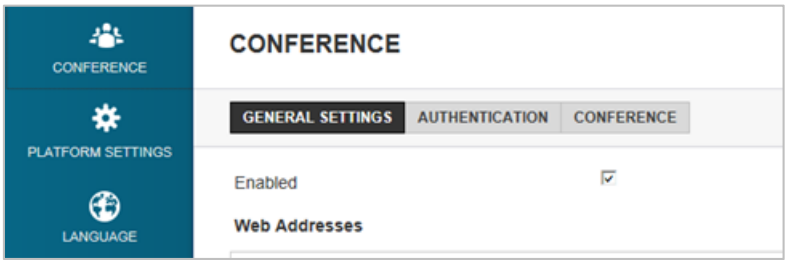
Set Up Licensing on the RealPresence CloudAXIS Experience Portal

After the licensing server is successfully configured and the licenses are activated on the RealPresence CloudAXIS Services Portal, you can set up a new RealPresence CloudAXIS Experience Portal instance and direct it to the RealPresence CloudAXIS Services Portal to obtain licensing.

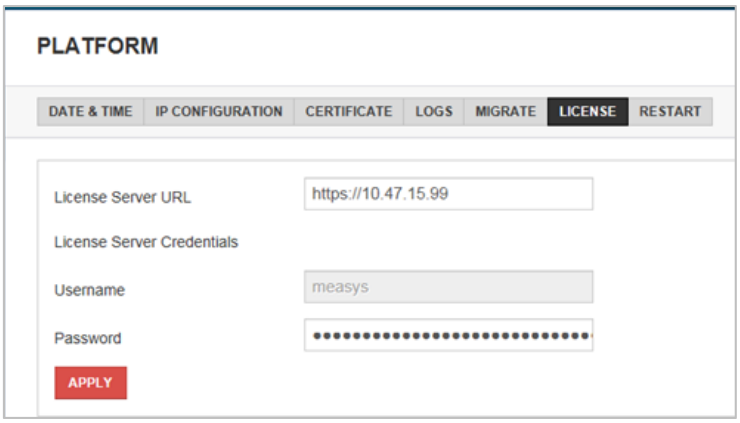
To set up licensing for the RealPresence CloudAXIS Experience Portal within Platform Director:

1. Set up and configure a new Experience Portal instance per the instructions in the *Polycom RealPresence Platform Director Administrator Guide* for creating a new software instance.
2. Log into the administrator interface for the new the Experience Portal using its FQDN and the port number 9445 for the Experience Portal admin interface.

   For example, type *https://<experienceportal.domain.com>:9445*.
3. Change the Administrator password, if prompted.
4. In the Experience Portal administrator interface, click **CONFERENCE > GENERAL SETTINGS**.
5. Click the **Enabled** check box to enable conference settings, as shown next.



6. Click **PLATFORM SETTINGS > LICENSE**.
7. In the License Server URL text box, type the URL or secure IP address (*https://<xxx.xxx.xxx.xxx>*) for the associated Services Portal, as shown next.



8. Type the password for the **measys** system user that you set up when you created and configured the Services Portal instance. The default password is **measys**.
9. Click **APPLY**.

10 Click **PLATFORM SETTINGS > RESTART > REBOOT SERVER**.

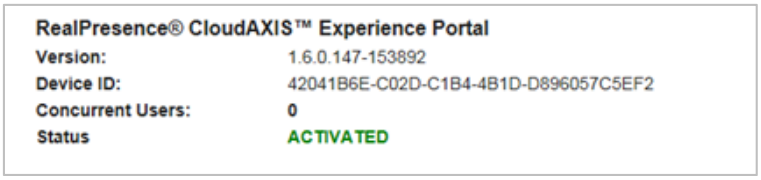
Rebooting the server associates the Experience Portal with the Services Portal and enables the Experience Portal to pick up licensing information from the Services Portal.

After the MEA instance reboots, you can log in to the Services Portal to verify the license settings.

11 From the Services Portal Administrator interface, click **PLATFORM SETTINGS > LICENSE**.

12 Verify the following license settings:

- The IP address for the **Licensing Server** should be the IP address for the Platform Director instance that manages this RealPresence CloudAXIS Services Portal.
- The Services Portal **License Information** section should reflect an activated license.
- The Experience Portal license is activated, as shown next.



Next, you can allocate licenses to the RealPresence CloudAXIS portals.

Allocate Licenses for RealPresence CloudAXIS Suite

The *Polycom RealPresence Platform Director Administrator Guide* provides instructions on allocating licenses for your RealPresence CloudAXIS Suite. You can allocate a number of MEA-ATTENDEES for the portal, which represents the number of concurrent users that are allowed to attend meetings through the RealPresence CloudAXIS Experience Portal at any time.

View RealPresence CloudAXIS Suite License Status

You can view the status of RealPresence CloudAXIS licenses on either portal at any time. The RealPresence CloudAXIS Services Portal tracks the activation status, version, unique device ID, and the total number of licenses allocated to the RealPresence CloudAXIS Suite instance. The RealPresence CloudAXIS Experience portal shows license details, including the product type and specific features as defined for the Polycom RealPresence system.

To view license status in the RealPresence CloudAXIS Services Portal:

» From the Services Portal administrator interface, click **PLATFORM SETTINGS > LICENSE.**

To view license status in the RealPresence CloudAXIS Experience Portal:

» From the Experience Portal administrator interface, click **PLATFORM SETTINGS > LICENSE > DISPLAY LICENSE INFO**.

The RealPresence CloudAXIS Experience Portal pulls licensing information from the RealPresence CloudAXIS Services Portal, which pulls information from the Platform Director instance, so license updates can take up to an hour to display on the RealPresence CloudAXIS Experience Portal.

Activate Licenses for a Stand-Alone RealPresence CloudAXIS Suite

If your RealPresence CloudAXIS Suite operates in stand-alone mode outside of RealPresence Platform Director, you have to activate licenses through the RealPresence CloudAXIS Services Portal for both the RealPresence CloudAXIS Experience Portal and the RealPresence CloudAXIS Services Portal.

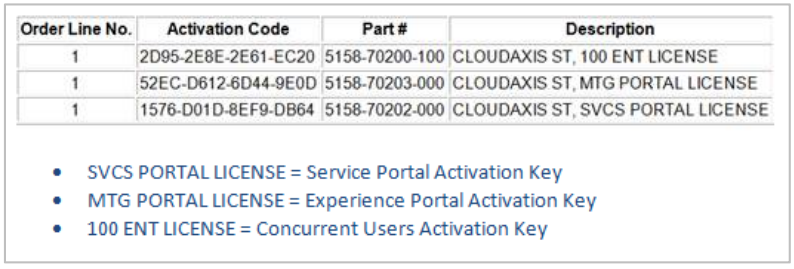
You can activate either license in one of the following modes:

- **Online mode** License information is sent directly to the Flexera license server for activation. The Services Portal must have Internet access to complete the activation.
- **Offline mode** A file is prepared and sent to Polycom so that the Flexera license server can activate the license and send back an activation file.

You must activate the RealPresence CloudAXIS Services Portal license, which is your RealPresence CloudAXIS Suite product license, before you can configure the RealPresence CloudAXIS Services Portal.

Make sure you have the activation keys available when you begin activating the RealPresence CloudAXIS Suite portals licenses. The activation keys were sent to you in an e-mail after your company purchased RealPresence CloudAXIS Suite, as shown in the following graphic.

Activation keys for RealPresence CloudAXIS Suite



Order Line No.	Activation Code	Part #	Description
1	2D95-2E8E-2E61-EC20	5158-70200-100	CLOUDAXIS ST, 100 ENT LICENSE
1	52EC-D612-6D44-9E0D	5158-70203-000	CLOUDAXIS ST, MTG PORTAL LICENSE
1	1576-D01D-8EF9-DB64	5158-70202-000	CLOUDAXIS ST, SVCS PORTAL LICENSE

- SVCS PORTAL LICENSE = Service Portal Activation Key
- MTG PORTAL LICENSE = Experience Portal Activation Key
- 100 ENT LICENSE = Concurrent Users Activation Key

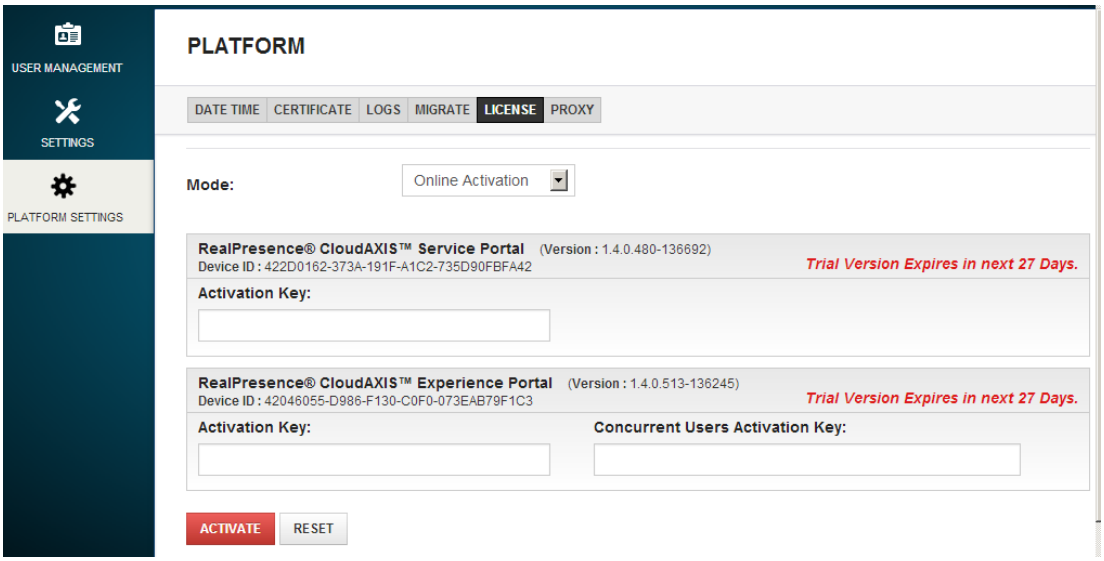
Activate Licenses in Online Mode

Activating licenses in online mode requires Internet access to communicate directly with the Flexera license server.

To activate the Services Portal and Experience Portal licenses in online mode:

1. Open your Services Portal and log in with Super Admin credentials.
2. Click **PLATFORM SETTINGS > LICENSE**.

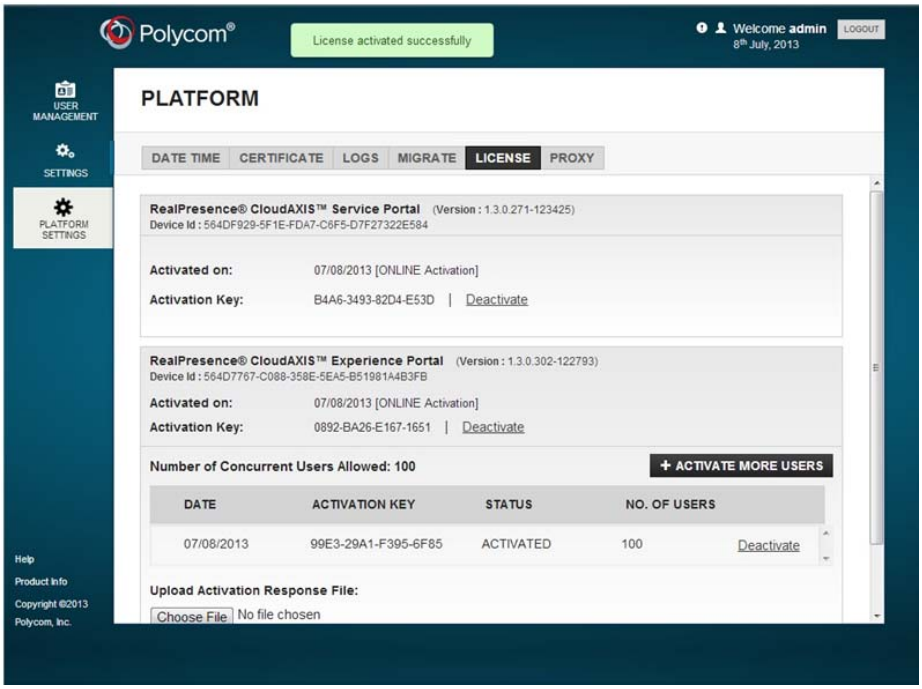
   The **License** screen displays with license information for the Services Portal and the Experience Portal.



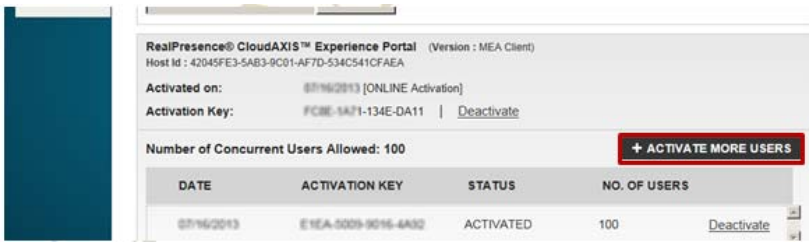
3 Enter your activation keys in the **Services Portal Activation Key**, **Experience Portal Activation Key**, and **Concurrent Users Activation Key** fields.

4 Click **ACTIVATE**.

The screen refreshes, a message indicates the license activation was successful, and a list of activated licenses are displayed, as shown next.



5 Click **+ ACTIVATE MORE USERS** to activate an additional 100 users.



Activate Licenses in Offline Mode

You can activate licenses for the Services Portal and Experience Portal in offline mode. First, complete the following procedure to activate licenses for the Services Portal. Repeat the procedure to activate licenses for the Experience Portal.

To activate Services Portal or Experience Portal licenses in offline mode:

1. In the Services Portal, click **PLATFORM SETTINGS > LICENSE**.
2. From the **Mode** drop-down menu, click **Offline Activation**.
3. Enter the corresponding activation keys for the portals:
   - For the Services Portal, enter the activation key in the **Services Portal Activation Key** field.
   - For the Experience Portal, enter the activation keys in the **Experience Portal Activation Key** and **Concurrent Users Activation Key** fields.
4. Click **Download Activation Request File** for the Services Portal or Experience Portal.

   A .bin file is sent to your computer, and the activation request file downloads.
5. Log in to the RealPresence CloudAXIS Suite Licensing Center with your credentials.
6. Click **Upload Capability Request** from the left menu.
7. On the **Upload Capability Request** screen, click B**rowse**, find the .bin file that was downloaded, and click **SEND**.

   The Flexera system responds by sending back the **response.bin** file.
8. Save the .bin file to your local computer.
9. In the Services Portal, click **Choose File** under **Upload Activation Response File** and find the .bin and upload your activation response file.
10. Click **ACTIVATE** to activate the Services Portal or Experience Portal licenses.

    A message displays stating that the license is activated.

Caution: Configure the RealPresence CloudAXIS Experience Portal license URL first

The RealPresence CloudAXIS Experience Portal license URL must be configured before setting RealPresence CloudAXIS Experience Portal licenses on the RealPresence CloudAXIS Services Portal.

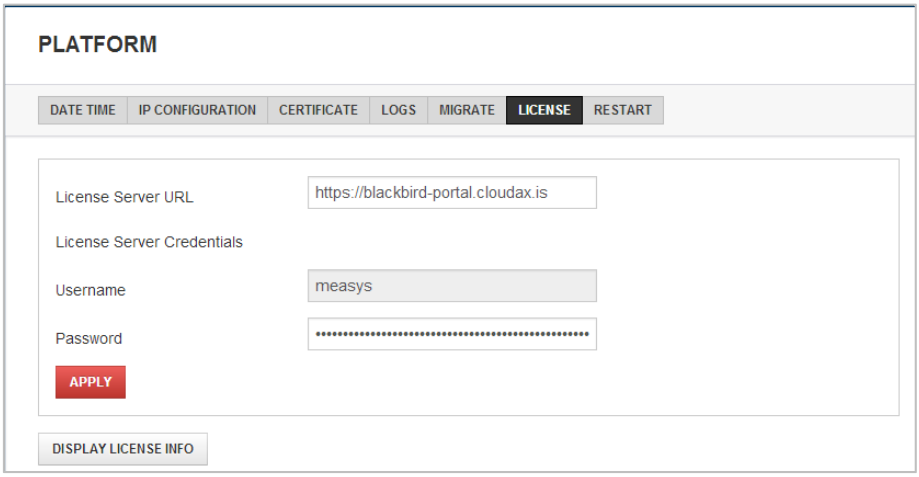
Activate the RealPresence Experience Portal Connection

After you activate the RealPresence CloudAXIS Suite portal licenses, you need to activate the connection between the RealPresence Experience Portal and the RealPresence Services Portal.

To activate the Experience Portal connection to the Services Portal:

1. Log in to the Experience Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > LICENSE**.

   The license information displays.



3. In the **License Server URL** field, enter the URL of the Services Portal used to procure your licensing information.
4. In the **License Server Credentials** fields, enter the **Username** and **Password** used to access the License Server. The default username and password are **measys**/**measys**.
5. Click **APPLY**.

To view the license information in the RealPresence CloudAXIS Experience Portal:

1. Log in to the Experience Portal with Super Admin credentials.
2. Click **PLATFORM SETTINGS > LICENSE**, and click **DISPLAY LICENSE INFO** to display information regarding Experience Portal Licenses.

Deactivate Licenses

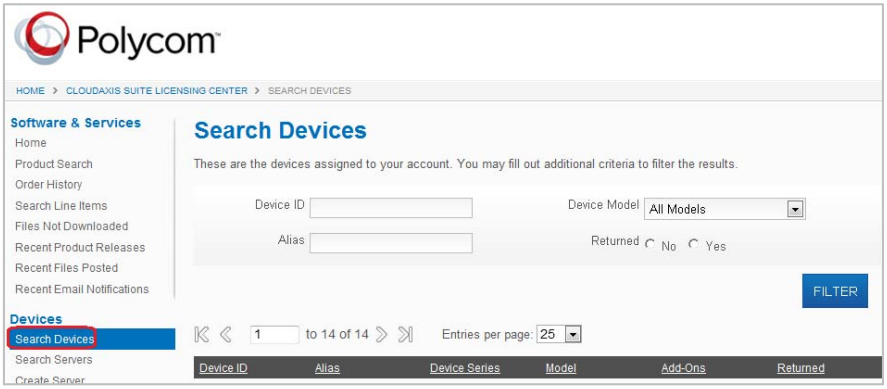
Each listed activation key includes a Deactivate option next to the license number. To reuse a license on a new instance, you must first deactivate it on the old instance. You can deactivate licenses in online or offline mode.

To deactivate a RealPresence CloudAXIS Services Portal license in online mode:

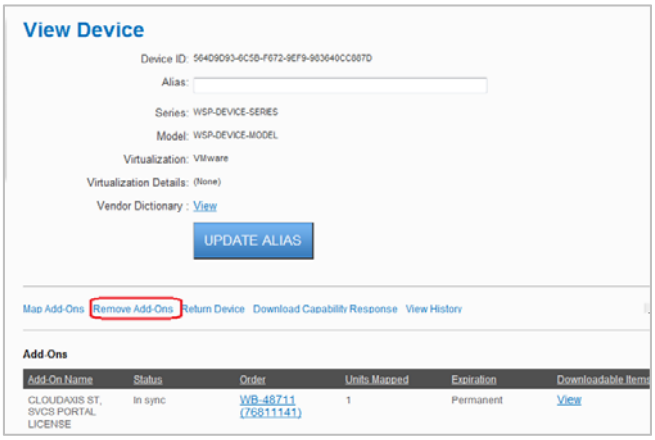
1. On the **Platform License Settings** page, click **Deactivate** next an active license you want to deactivate.
2. Call Polycom Support to generate another activation key with another device ID.

To deactivate the Services Portal or Experience Portal license in offline mode:

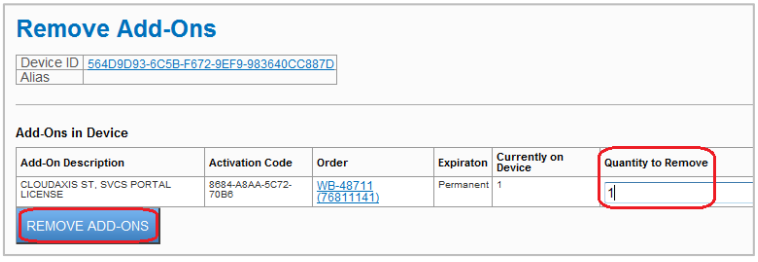
1. Call Polycom Support to receive a Deactivation Response File.
2. Download the Deactivation Response file from the RealPresence CloudAXIS Suite Licensing Center.
3. On the left toolbar under **Devices**, select **Search Devices**, as shown next.



4. Look for the device ID of the system that you are deactivating. Select that device ID to open the **View Device** screen, shown next.



5. Click **Remove Add-Ons** to open the **Remove Add-Ons** screen, as shown.



6. In the **Quantity to Remove** field, enter **1**; then click **REMOVE ADD-ONS**.
7. On the **View Device** screen, click **Download Capability Response**.

8 Open the Services Portal or Experience Portal license page and click **Deactivation**.

9 In the **Upload Deactivation Response File** drop-down menu, click the response file that you acquired in step 7.

10 Click **YES**.

A message indicates that deactivation was successful.

Secure Shell and Restricted Shell Commands

The Polycom RealPresence CloudAXIS Restricted Shell provides a means for you to log in to RealPresence CloudAXIS Suite from either a console or a Secure Shell (SSH) connection. You can connect to the shell through the vSphere console or with an SSH client using the FQDN or IP address that was set up for either the RealPresence CloudAXIS Services Portal or the RealPresence CloudAXIS Experience Portal.

The user accounts *caxis* and *polycom* were set up in the system to perform network shell operations within the shell. Both accounts were set up in the system with *caxis* or *polycom* as the default password. Polycom requires you change these passwords when you first connect to the shell.

The shell supports basic Linux commands including `cat`, `find`, `grep`, `pwd`, `vi`, `scp`, `tail`, `cd`, `echo`, and `exit`.

The following table outlines the operations that you can perform from the shell.

Restricted Shell Operations

Operation	*Shell Command*	*Notes*

View status of web services	`services nginx status`
	`services tomcat6 status`
	`services –status -all`
		Show status for the nginx and tomcat web services to determine whether they are running. When these services are not running, users cannot access the web portals.

Start web services	`services nginx start` `services tomcat6`	Use the start command to start services that are not running. Do not use it for services that are in a running state.
Restart web services	`services nginx restart` `services tomcat6 restart`	Use the restart command to restart web services that are running.
Change system hostname	`change_hostname`	Upon entering the command, the current hostname is shown, along with a prompt asking whether you want to change the system hostname. Type the new hostname exactly as you want it to display in your system. A message tells you the name was changed successfully.
Change the password for the *caxis* and *polycom* users	`change_password`	Change the password while you are logged in to the shell. For security reasons, the system does not display the new password but does indicate that the password has been changed successfully.

Operation	*Shell Command*	*Notes*
Configure or change NTP settings	`change_ntp`	The command displays a list of NTP servers that have been configured in the system. Follow the system prompts to specify the new time servers to be added to the system.
Synchronize system date and time with a specific NTP server	`ntupdate –u <fully qualified dns name or IP address of the NTP server>`	The system indicates that the time has been adjusted.
Set or change system date and time	`change_system_datetime`	Follow the system prompts, and then enter the date and time in the following format: Day Month Date Hour:Minute:Second Zone Year. For example: **`Mon Jun 17 20:27:27 UTC 2013`** `The system indicates when a time and date change has been successful.`
Change the time zone for the system	`change_timezone`	The current time zone is displayed. Follow the prompts to change the zone, and press the return key to display a list of sorted time zones from which to choose. Note that the time zone can be changed within the Administrator interface for either RealPresence CloudAXIS portal.
View system network information	`show_network_info`	All relevant network settings, including IP configuration, DNS domains, and servers are displayed. Use this command to determine the current network configuration or verify that newly made network changes are correct.
Change network settings	`change_network_settings`	Use this command to change network settings from their current state. The options available depend upon the current network configuration. With this command, you can: • enable or disable DHCP • enable or disable static IP • configure static IP settings • change DNS settings • restart network services for the new settings to take effect Follow the prompts to change the settings you want to change.

Operation	*Shell Command*	*Notes*
Reboot the system	`reboot`	The *reboot* command stops and restarts the entire system. Use with caution.
Exit the restricted shell	`exit`	
Show the current product version	`show_product_info`	The version/build number of the Services Portal or Experience Portal is displayed.
Regenerate trust certificates	`regenerate_certificates`	A message shows that the certificates have been regenerated successfully. Follow the prompts to restart the web services to apply the new certificate settings. Note that certificates can be regenerated within the Administrator interfaces for the Services Portal and Experience Portal.

Recommendations for Secure Access

The section provides information on providing invited guests and remote users with controlled access to your organization's unified communications infrastructure while preventing unwelcomed intrusion.

Secure Web Access

To provide conference access to guest users joining from outside your organization's firewall, they must be able to access the RealPresence CloudAXIS Experience Portal from the Internet. Access to the RealPresence CloudAXIS Services Portal, however, is required only for users who create and host conferences, and who are typically members of your organization. Providing direct external access to the RealPresence CloudAXIS Services Portal component is left to the administrator's discretion.

The following options can be used to provide access from external networks:

- Configure NAT functionality in your organizational firewall, or another edge device, to map HTTPS port 443 from the external IP address assigned for the RealPresence CloudAXIS Experience Portal to its internal IP address. Do the same for the RealPresence CloudAXIS Services Portal (if desired).
- Use a reverse proxy product to provide external HTTPS access to the RealPresence CloudAXIS Experience Portal. Do the same for the RealPresence CloudAXIS Services Portal (if desired).

  The proxy selected should support the following features:

  - Forwarding of the Web Sockets protocol (RFC 6455)
  - Traffic routing based on HTTP host headers. This is required only when you want to route a single external IP address to multiple internal web applications. In this case, multiple DNS records (such as meet.contoso.com and schedule.contoso.com) can be configured to point to the same IP address; the reverse proxy forwards web traffic to the appropriate IP address based on the host name in the HTTP request header.

  The Polycom RealPresence Access Director (RPAD) product versions 3.0 and higher can be configured to perform this function. For more information, see the "Working with Access Proxy Settings" section of the *Polycom RealPresence Access Director System Administrator Guide*.

Tunnel Access for Remote Users

Restrictive firewall policies on remote networks may block egress for UDP-based traffic, limit TCP egress to ports 80 and 443, and in some cases require that those ports be forwarded by a local proxy. To enable guest access for clients joining from such a restrictive network, you can enable the HTTPS Tunneling feature on RealPresence Access Director and define a tunnel access point (see Connect to a Polycom Access Point). If remote endpoints cannot establish a native SIP/RTP connection to the edge proxy (by accessing UDP port 5060), the signaling and media can be tunneled through HTTPS to the edge proxy. The result is that video and audio connectivity can be established from restrictive remote network environments.

Limitations Associated with Tunneling

Tunneling in a restrictive firewall environment can include some of the following limitations:

- Tunneling requires that RealPresence Access Director version 3.1 or later be used as the tunnel access point. Third-party edge proxy products such as Acme Packet cannot serve this function.
- Sending and receiving shared content for tunneled endpoints requires that RealPresence Access Director version 4.0 or later be used as the tunnel access point.
- SVC-style calls are not supported over HTTP tunnels. If a RealPresence CloudAXIS endpoint makes a tunneled connection to a conference that is configured for Mixed AVC and SVC, the tunneled client uses AVC for the call. If a RealPresence CloudAXIS endpoint makes a tunneled connection to a conference that is configured for SVC-only, the call fails.
- A tunneled access point is typically subject to a lower maximum call rate than a non-tunneled client. The maximum call rate for tunneled access points is 512 kbps.
- If the RealPresence CloudAXIS Suite client determines that network bandwidth or quality is insufficient to allow for high-quality video to be sent across the tunnel, the connection automatically falls back to audio-only mode. This change can occur upon joining the conference or while it is in progress.
- Some web proxies may perform a deep inspection of traffic being tunneled through the proxy. In some cases, the web proxy may block the tunneled call. In this case, an exception may need to be added to the web proxy to allow tunneled connections to the RealPresence Access Director. For details on adding exceptions to a web proxy, consult the web proxy manufacturer's documentation or support.
- Some web proxies require the user to be authenticated in order to traverse them.
  - In the case of explicit web proxies, where RealPresence CloudAXIS Suite is aware of the web proxy via the web browser’s configuration, the RealPresence CloudAXIS Suite plug-in can participate in this authentication process.
  - In the case of transparent web proxies, where RealPresence CloudAXIS Suite is not aware of the web proxy via the web browser’s configuration, the RealPresence CloudAXIS Suite plug-in cannot provide authentication to the transparent web proxy. In this case, the tunneled call attempt will fail. Check the web proxy manufacturer's documentation or support for possible workarounds to this problem.
- If the RealPresence CloudAXIS Suite solution is configured to support tunneled calls, it is important that the RealPresence DMA system's configuration allows SIP UDP connections for internal users. This is necessary in order to support the CloudAXIS web client's detection of whether or not tunneled calls are required. Failure to ensure this results in unnecessary tunneled calls for internal users. Note that RealPresence CloudAXIS Suite uses TLS for SIP connections.

Refer to “Working with Access Proxy Settings” in the latest release version of *Polycom RealPresence Access Director System Administrator Guide* for more information.

Note: Certificates for HTTPS Proxy with the RealPresence CloudAXIS Experience Portal

If you add host-header next hops, you must specify the host FQDNs as Subject Alternative Names (SANs) in the Certificate Signing Request for the RealPresence Access Director system.

Secure SIP Access for Guests

Enabling SIP guest access is the most convenient way to allow video and audio access from organizations and individuals that are not federated with your organization. For this reason, the RealPresence CloudAXIS web client functions by default in a guest mode; it neither registers nor authenticates itself with your organization's SIP gatekeeper, which is typically a Polycom RealPresence DMA system. This may be true even if the RealPresence DMA system is used by individuals who belong to your organization and/or connect from within your organizational firewall.

Similarly, RealPresence Mobile, with SIP registration and authentication capabilities, does not register or authenticate with the target SIP gatekeeper when it joins a conference in response to the user clicking on the **Join Now** button from the RealPresence CloudAXIS Experience Portal.

You can enable authenticated SIP access for verified members of your organization by configuring the SIP username and password information in the RealPresence CloudAXIS Services Portal RealPresence DMA settings. When authenticated SIP access is enabled, these credentials are automatically and securely provided to supported endpoints for the members of your organization who have authenticated to the RealPresence CloudAXIS Services Portal web interface. Supported endpoints include the RealPresence CloudAXIS Suite and Polycom RealPresence Mobile v3.1 and above, which attempt to authenticate to the SIP gatekeeper, if challenged, using the supplied credentials. Users benefit from authenticated dialing, which may include access to a less restrictive dial plan.

Guest users who have not authenticated to the RealPresence CloudAXIS Suite Services Portal, but are supplied an external e-mail address when attempting to join a meeting, are not provided SIP credentials. They are instead always dialed in as unauthenticated SIP callers subject to the dialing rules for unauthenticated endpoints.

Because the RealPresence CloudAXIS Suite typically functions in guest mode, RealPresence CloudAXIS Suite requires SIP guest access for external users wanting to join meetings via the RealPresence CloudAXIS Experience Portal. You can also provide H.323 guest access at your discretion to facilitate access from other types of endpoints.

Edge Proxy Access for Guests

To enable guest access across your organization's edge proxy device, refer to one of the following Polycom publications. Follow the recommendation for enabling endpoint authentication on the applicable RealPresence DMA system as described in these guides.

- See "Deploying the Basic RealPresence Access Director System Solution to Support Remote and Guest Users" in *Deploying Polycom Unified Communications in RealPresence Access Director™ System Environments*.
- See "Deploying the Polycom—Acme Packet Solution to Support Remote and Guest Users" in *Deploying Polycom Unified Communications in an Acme Packet Environment.*

Edge proxies, including RealPresence Access Director, may require authenticating and non-authenticating callers distinguish themselves by sending SIP requests to a different port or by using a special dialing prefix. To configure these settings, specify the correct Authentication Mode when configuring access points in the RealPresence CloudAXIS Services Portal (see Connect to a Polycom Access Point). It may be necessary or desirable to specify two different access points corresponding to the same edge device, one for AUTH users and one for NoAUTH users, with each access point entry specifying a different port number and/or dial prefix to use for the corresponding access case.

Additional Recommendations to Increase Security

Follow these recommendations to secure the privacy of your conferences and to prevent misuse of your videoconferencing infrastructure:

- Use temporary rather than persistent (personal) VMRs when creating meetings that include untrusted guests. This is the default RealPresence CloudAXIS Services Portal behavior used whenever the Use Personal VMR has not been checked on the Schedule a Meeting screen. Using temporary VMRs helps ensure that guests are able to access only the particular conference session you are inviting them to.

  See the *Polycom RealPresence CloudAXIS Suite User Guide* for additional information.

- Select the **Require Authentication** check box on the **Schedule a Meeting** screen to provide an additional level of access control.
- Select the **Generate VMR from Range** check box on the RealPresence CloudAXIS Services Portal DMA CONFIG tab to generate temporary conferencing IDs in a wide, random range. This action makes the IDs more difficult to access by random dialing. See Connect to a Polycom Access Point.
- Restrict guest users to a subset of your dialing plan. By provisioning a dialing rule for unauthorized calls on your RealPresence DMA system, you can limit guests to particular dial identifiers or ranges for which you prefer to provide access. For example, the following preliminary script restricts guest users to the dial ID range of 100,000 to 999,999, which could be configured to be the same auto-generation range used by the RealPresence CloudAXIS Services Portal to create temporary VMRs.

```
// These values should correspond to the min and max room ID settings
// specified in the RealPresence CloudAXIS Services Portal DMA Config
Option "Generate VMR
// From Range"

var maxGeneratedRoomId = 100000;
var maxGeneratedRoomId = 999999;

var number  = parseInt(DIAL_STRING.replace(/^sip:([^@]*)@?(.*)/i,"$1"));
if (NaN != number && number > minGeneratedRoomId && number <
maxGeneratedRoomId){
   return;
}
return NEXT_RULE;
```

Web Info: Configuring dialing scripts on DMA 7000

For more instructions on how to configure preliminary dialing scripts on the RealPresence DMA system, see the *Polycom RealPresence DMA System Operations Guide*.

Troubleshoot Issues

This section shows you how to resolve issues with RealPresence CloudAXIS Suite and how to access log files for troubleshooting miscellaneous issues.

Portal URL (FQDN) is unresponsive

Operating the RealPresence CloudAXIS Services Portal requires that nginx and Apache Tomcat services run on the server. Unresponsive web addresses can indicate that those services are not running. If the RealPresence CloudAXIS Services Portal URL does not respond when you attempt to open it in a web browser, open the RealPresence CloudAXIS Services Portal login screen and confirm that the nginx server and the Apache server are running.

To confirm that the nginx and Apache services are running:

1. Using the vSphere console, or by connecting via an SSH client to the Services Portal FQDN, open the Services Portal console.
2. Log in using **caxis** for both your **Username** and **Password**.
3. View the status by entering one of the following commands:
   - Enter **`service nginx status`** for the nginx status.
   - Enter **`services tomcat6 status`** for the Apache status.
   - Enter **`service –status-all`** for the status on all servers.

Start servers if they are not running, and restart them if they are running but you are still having problems with the link

To start or restart servers:

» Do one of the following:

- To start servers, enter the following commands:
  - **`services nginx start`**
  - **`services tomcat6 start`**
- To restart servers, enter the following commands:
  - **`services nginx restart`**
  - **`services tomcat6 restart`**

User cannot create meetings

If users are unable to create a meeting, confirm the following on the RealPresence CloudAXIS Services Portal:

- At least one RealPresence DMA system is made primary.
- The RealPresence DMA system owner's username entered in the RealPresence CloudAXIS Services Portal also exists in the RealPresence DMA system. For information on how to create a username for the RealPresence DMA system, see the *Polycom RealPresence DMA 7000 System Operations Guide*.

- The RealPresence DMA system status is up.

User cannot launch the Welcome screen

The Welcome screen displays video options for entering the meeting. If users can create a meeting but cannot launch the welcome screen, confirm that the correct port numbers and RealPresence DMA system FQDN have been configured in the RealPresence CloudAXIS Experience Portal (see Connect to a Polycom Access Point).

Configured components do not respond

If all components are correctly configured but not working, reboot the RealPresence CloudAXIS Services Portal server then reboot the RealPresence CloudAXIS Experience Portal.

Super Admins and Admins cannot add Active Directory users

If the RealPresence CloudAXIS Services Portal admin and Super Admin are unable to add an Active Directory user, confirm that the proper LDAP server is configured with the correct values listed in Set Up LDAP Authentication.

Both the RealPresence CloudAXIS Services Portal and the RealPresence CloudAXIS Experience Portal must be configured to the same time zone and NTP server in order for RealPresence CloudAXIS Recording to work properly.

To configure the same time zone and NTP server:

1. Access the CLI on either of the two portals, using **caxis** as both the **Username** and **Password**.
2. Select your time zone by entering the CLI command `change_timezone`.
3. Sync your server with the NTP server by entering the CLI command `ntpdate`.
4. Repeat steps 1–3 on the other portal.

If the problem persists, contact your IT administrator to confirm that the values are correct.

User cannot send e-mail notifications

If users are unable to send e-mail notifications, confirm that the proper SMTP server is configured with the correct port numbers listed in Enable E-mail Notifications for Users. If the problem persists, contact your IT administrator to confirm that the values are correct.

User receives error message: “Unable to create a conference with a personal VMR”

Confirm that the virtual meeting room exists on the configured RealPresence DMA system. If it exists, contact Polycom Support.

Also, check the RealPresence CloudAXIS Services Portal configuration to confirm that the administrator username and password account set up for the RealPresence DMA system is authorized as an Active Directory administrator on the RealPresence DMA system. A local administrator cannot see Active Directory users.

User receives message: “External server not set”

If the user receives the “External Server Not Set” message after selecting Meet Now, confirm that the correct FQDN is entered into the MEA Server text box located on RealPresence CloudAXIS Services Portal’s Server Settings screen (see RealPresence CloudAXIS Services Portal Server Settings).

User Receives message: “Resources are not available”

This error message displays if the license trial period has ended or when the concurrent license limit is exceeded. Contact your Polycom representative to purchase a license to activate your RealPresence CloudAXIS Suite or to increase your user capacity.

Administrator cannot download log files with Internet Explorer

If an administrator cannot download logs using Internet Explorer, follow the steps provided on the user interface, and retry loading the logs.

User cannot see all participants in the Roster

If a user cannot see all the participants in the roster, verify that the dial prefixes for the RealPresence DMA system are the same on the Services Portal and Experience Portal, and verify the RealPresence DMA system password configured on the Experience Portal is correct.

Single Sign-On (SSO) is not working

The following table includes a list of reasons why SSO may not be working properly with possible solutions for each.

SSO Issues and Solutions

Problem	*Solution*
RealPresence CloudAXIS Suite could not obtain a Kerberos ticket from the domain. This can happen if the domain is temporarily unavailable. For example, when you’re connected to the network with VPN or on a laptop with multiple network interfaces that do not include the correct Windows domain.	Check your network settings and temporarily disable unused interfaces.
Integrated Windows authentication is not enabled.	In Internet Explorer, click **Tools > Internet Options > Advanced**. Select **Enable Integrated Windows Authentication**, click **Apply**, and restart Internet Explorer.
There is an issue with the Kerberos service principal and RealPresence CloudAXIS Suite results to trying the NT LAN Manager (NTLM). This occurs if the targeted Service Principal Name (SPN) is not set on the HTTP service account or if there are multiple service accounts with the same SPN.	See Set a Service Principal Name for the Services Portal User Account in Active Directory.

Problem	*Solution*
The HTTP service account is disabled.	
If you enter your credentials into the Network Password dialog box, the browser will continue to submit network credentials using NTLM authentication even after you have resolved the issue with the network password.	Purge saved passwords. Click **Start > Control Panel > User Accounts > Manage User Accounts > Advanced > Manage Passwords**, and make sure there are no passwords saved for the target site.
The time synchronization on the servers are out of sync.	Synchronize the time on the servers using the NTP serve (see Set the Time Zone and NTP Server) and check that the times regularly (see Verify the Time Settings).

SSO authentication has failed

The SSO feature in the RealPresence CloudAXIS Services Portal is provided by a separate bundle in a war package. When authentication fails, a set of error and debug messages, if enabled, are logged. You can trace the issues with SSO Authentication with the following log patterns in the log file `/var/log/tomcat6/cloudaxis_wsp-ui.log`.

The following are common debug messages that are logged when SSO fails. An explanation follows each log pattern.

Debug Message 1

```
KDC has no support for encryption type (14) OR
Cannot find key of appropriate type to decrypt AP REP - RC4 with HMAC OR
Cryptographic key type rc4-hmac not found OR
Cryptographic key type des-cbc-md5 not found OR
Cryptographic key type des-cbc-crc not found OR
```

Explanation:

These errors mean that the identity of the domain user account does not have the **Use DES Encryption types for this account** option set if DES security is desired or that it has the option set for if RC4-HMAC security is desired. The errors could also mean that the wrong keytab utility was used to generate the keytab file. For example, the Sun keytab was used on a WebSphere system. See Generate a Keytab File for the Services Portal User for information on generating a keytab file.

Debug Message 2

```
org.ietf.jgss.GSSException: Defective token detected (Mechanism level:
GSSHeader did not find the right tag)
```

Explanation:

There are a variety of conditions that could cause Kerberos authentication to not work and cause RealPresence CloudAXIS Suite to fall back to NTLM. The following include general reasons for no or invalid Kerberos service tickets being sent to the Services Portal server:

- ***Duplicate Service Principal Names (SPNs)*** SPNs need to be unique. Remove all duplicate SPNs, create a new SPN for the service account, generate the keytab file again, and update the SSO Configuration with the new keytab file.
- ***The user is logged in outside of the domain*** In order to get a Kerberos ticket, the user must initiate a login within the domain. If a user does not login with the domain before starting the SSO, they won't have a ticket to send when the adapter asks for it. The Microsoft client must also be joined to the domain. If the client is not joined, it cannot participate in Kerberos authentication and thus the client has no choice but to fallback to using NTLM.
- ***Incorrect Browser Configuration*** The browser must be configured to trust the target server to send the credentials. In Internet Explorer, you must add the target server or it's domain under. Click **Tools > Internet Options > Security > Intranet Zone**. Make sure it is Intranet Zone. Integrated Windows Authentication must also be turned on for automatic authentication in some browsers. In Internet Explorer, click **Tools > Internet Options > Advanced** and select **Enabled Integrated Windows Authentication**.
- ***Outdated Windows Login*** After setting the SPN, users who use SSO need to re-enter their credentials to authenticate to the domain controller. By providing their credentials, they get a new ticket with the SPN changes. Make sure to logout and re-login into the AD domain.
- ***Outdated Saved Network Credentials*** If the user entered and saved credentials into a Network Password dialog box, it prompts the client to initiate NTLM rather than Kerberos.
- ***SPN in general*** There is a problem with the SPN on the service account or domain user account preventing the client from initiating Kerberos authentication and thus the client has no choice but to fallback to using NTLM.
- **RealPresence CloudAXIS Services Portal is running on the same machine as the domain controller** This should never be a scenario in a Services Portal deployment.
- ***DNS Hostname*** Make sure the Services Portal URL hostname is a DNS A record hostname instead of CNAME alias. When the browser requests a ticket from KDC, it always uses the DNS A record hostname, regardless of the hostname you have in browser address bar. Users can still use CNAME alias hostnames to access the site, but the keytab must be created using a record hostname.

Debug Message 3

```
org.ietf.jgss.GSSException: Failure unspecified at GSS-API level (Mechanism
level: Clock skew too great (37)) OR
sun.security.krb5.internal.KrbApErrException: Clock skew too great (37)
```

Explanation:

The times on the servers are not synchronized with a NTP service (see Verify the Time Settings).

Appendix 1: Set Up Windows Active Directory for Single-Sign-On

Before setting up the Single Sign-On (SSO) configuration in the RealPresence CloudAXIS Services Portal, complete the following steps in your Active Directory server:

To prepare your Active Directory server for SSO:

1. Create a RealPresence CloudAXIS Services Portal User Account in Active Directory
2. Set a Service Principal Name for the WSP User Account in Active Directory
3. Generate a Keytab File for the WSP User

In addition, SSO requires trust certificates to operate in the RealPresence CloudAXIS web environment. If you have not already set up signed trust certificates for the RealPresence CloudAXIS Services Portal and Experience portal, see Manage Trust Certificates and Certificate Signing Requests before continuing with the single sign-on configuration.

Note: Only signed certificates are supported with SSO

Trusted, signed certificates must be used with SSO. Self-signed certificates are not supported in RealPresence CloudAXIS Suite.

To set up trust certificates in your server environment to support SSO:

1. Configure both the Services Portal and Experience Portal with signed CA certificates issued by a trusted CA authority (see Manage Trust Certificates and Certificate Signing Requests).
2. Configure Users' Internet Browsers to Use SSO.

Create a RealPresence CloudAXIS Services Portal User Account in Active Directory

To enable the RealPresence CloudAXIS Services Portal to recognize your Active Directory domain and authenticate users with single sign-on, you must create a user for the RealPresence CloudAXIS Services Portal in your Active Directory domain.

To create a RealPresence CloudAXIS Services Portal user in Active Directory:

1. Log in to the appropriate Windows Active Directory domain with administrator credentials.
2. Click **START > Control Panel > Administrative Tools > Active Directory Users and Computers**.
3. Create a user account for the Services Portal service.

Polycom recommends, though does not require, that the user account name be the same as the DNS host name of the RealPresence CloudAXIS Services Portal server.

4 Set a password for the Services Portal user account. Make note the password, as it is required in a later instruction.

Set a Service Principal Name for the Services Portal User Account in Active Directory

After creating the Active Directory user account for the RealPresence CloudAXIS Services Portal, you must add a servicePrincipalName value in the User Properties settings. The Service Principal Name (SPN) uniquely identifies the service instance for the RealPresence CloudAXIS Services Portal user account.

To set a Service Principal Name for the Services Portal user account:

1 In the Windows Active Directory domain server, click **START > Control Panel > Administrative Tools > ADSI Edit**.

2 Find the Services Portal user you created.

3 Open the user properties, and update the **servicePrincipalName** in the format of HTTP/<*wsp host name*>.<*AD domain name*>@<*AD DOMAIN NAME*>.

For example, where the WSP host name is *wsp-sso* and the Active Directory domain is *cloudax.is*, the servicePrincipalName would be *HTTP/wsp-sso.cloudax.is@CLOUDAX.IS*.

Polycom recommends that the Services Portal server and Active Directory server be located on the same Active Directory domain. However, if your network setup requires that they be located on different domains, SSO can be configured with the **servicePrincipalName** as HTTP/<*wsp_server_fqdn*>@<*AD_DOMAIN*>.

If the RealPresence CloudAXIS Services Portal server is part of domain1.com and AD domain is domain2.com, the **servicePrincipalName** format would be HTTP/<*wsp-sso.domain1.com*>@<*DOMAIN2.COM*>.

Note: Use the syntax and case exactly as displayed in the examples.

4 Save the updated user settings.

Generate a Keytab File for the Services Portal User

A keytab file contains principals and encrypted keys that allow users and scripts to authenticate with an enterprise domain without entering credentials. You must generate a keytab file on the Active Directory server for the RealPresence CloudAXIS Services Portal service and reference it in the RealPresence CloudAXIS Services Portal configuration settings. This file is used in the following procedures to enable single sign-on for the RealPresence CloudAXIS Services Portal.

Refer to the Ktpass page on the Windows Server Library site.

Caution: Follow appropriate security precautions when handling the keytab file

Because the keytab file contains highly secure information, keep it protected using very strict file-based access control to ensure that only designated administrators can read the file.

To generate a keytab file for the RealPresence CloudAXIS Services Portal user:

1. Log in to the Windows Active Directory domain as a domain administrator.
2. Open the command prompt, and execute the following command:

   `ktpass /out c:\`*`[WSP host name].[domain name]`*`.keytab /mapuser `*`[WSP host name]@[domain name]`* `/princ HTTP/`*`[WSP host name].[domain name]@[ DOMAIN NAME]`* `/pass `*`[WSP User Password]`* `/ptype KRB5_NT_PRINCIPAL /kvno 0 /crypto all`

   For example, where the WSP host name is *wsp-sso*, the user password is *Polycom123*, and the Active Directory domain is *cloudax.is*, the command would be as follows:

   `ktpass /out c:\wsp-sso.cloudax.is.keytab /mapuser wsp-sso@CLOUDAX.IS /princ HTTP/wsp-sso.cloudax.is@CLOUDAX.is / pass Polycom123 /ptype KRB5_NT_PRINCIPAL /kvno 0 /crypto all`

   Use the syntax and case exactly as they display in the example.
3. Verify that the keytab file (*[WSP host name].[AD domain name].*keytab) was created at the server root directory (c:\).

   Using the preceding example, the keytab file name would be *c:\wsp-sso.cloudax.is.keytab*.

Appendix 2: Create Apps to Use with Social Media Contacts

An administrator can set up the RealPresence CloudAXIS environment so that users can invite meeting participants from their personal Google+ accounts. Before setting up social policies to accommodate these social media contacts, you must create a customized app for either Google+ to connect user social networking contacts with the RealPresence CloudAXIS user environment.

Note: Facebook application creation is no longer supported

RealPresence CloudAXIS users no longer need to create a RealPresence CloudAXIS-enabled application to invite Facebook contacts because Facebook contacts are no longer supported. If you want to add Facebook contacts to a RealPresence CloudAXIS meeting, send them an invite by e-mail or send the meeting details in a message on Facebook.

You can create an application to enable access to Google+ contacts from the RealPresence CloudAXIS Services Portal. Follow the instructions in the following sections for more information on creating a Google+ application.

Before you begin, set up a neutral account with credentials that can be shared among different members in your team. Do not use your personal account to create the application, which helps to avoid dependencies on a single person. In case a person currently in charge of the application maintenance leaves the company, the common account credentials can be passed on to the team.

After you create the Google+ application, you must enable the Google+ application in the RealPresence CloudAXIS Services Portal. See Set Social Networking Policies for information on enabling your application.

In addition, always maintain one-to-one mapping between the RealPresence CloudAXIS Services Portal server and the application being used.

Create a Google+ Application

As you create your Google+ application, refer to the Google APIs Console Help website.

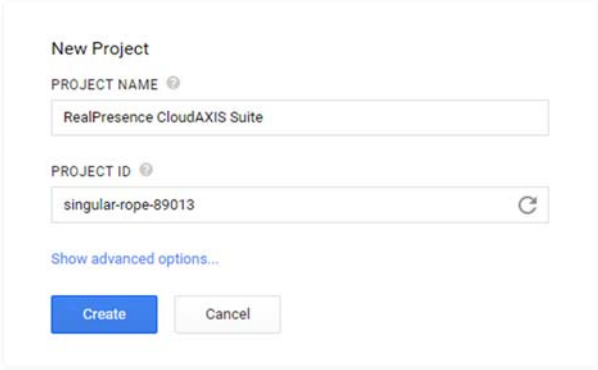
Note: IP address change

A change in the server's IP address does not require that you create a new application as long as the FQDN points to the changed IP address.

To create a Google+ application:

1. Log into the shared Google account.
2. Open the Google APIs Console page and click **Create Project**.

The **New Projects dialog box** is displayed, as shown next.

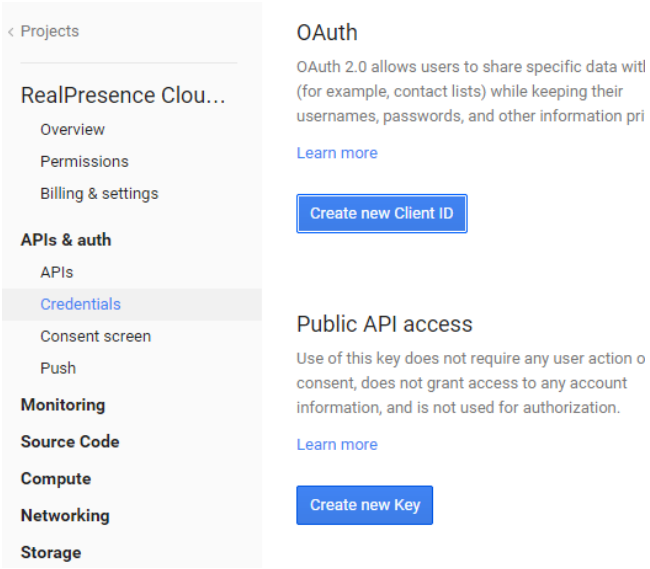


3 Enter a **Project Name** and click **Create**.

A notification with the name of the new project is displayed, and the project is added to your list of projects.

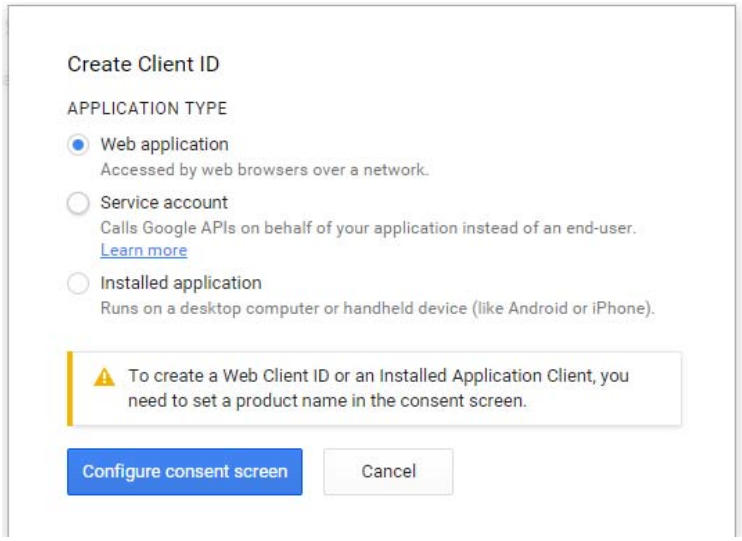
4 In **Projects**, click your project.

5 On left pane on the **Project Dashboard** page, click **APIs & auth > Credentials > Create new Client ID**, as shown next.



The **Create Client ID** dialog box is displayed.

6 Select **Web Application** and click **Configure consent screen**, as shown next.



7 Enter the following information:

- **Product name** Polycom recommends using a name with the prefix RealPresence CloudAXIS_.
- **Product logo** The URL to your product logo.
- **Home Page URL** The URL to your home page.
- **E-mail Address** The e-mail address for the shared Google account.

8 Click **Save**.

The **Create Client ID** dialog box is displayed.

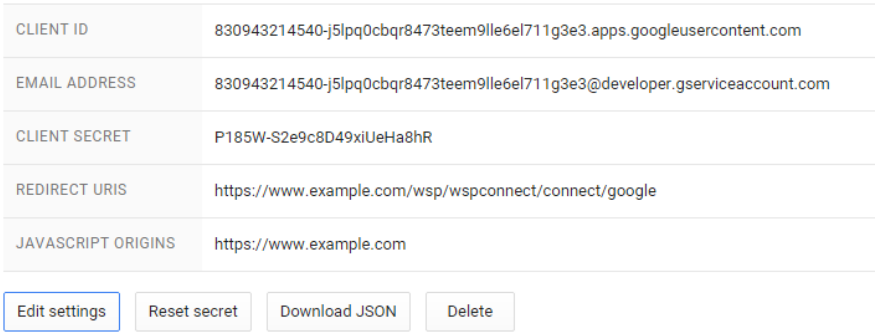
9 For **Application type**, select **Web application**.

10 For **Authorized JavaScript Origins**, enter the RealPresence CloudAXIS Services Portal's FQDN.

11 For **Authorized Redirect URIs**, enter **https://<*ServicesPortalFQDN*>/wsp/wspconnect/connect/google**.

12 Click **Create client ID**.

The **Client ID for web application** information is displayed, as shown next.



13 Make note of the **Client ID** and **Client secret** fields.

You need these two values to enable social networking contacts for Google+.

Note: Update redirect URL after migrating RealPresence CloudAXIS Suite to 1.7.x

If you previously created a Google+ application for RealPresence CloudAXIS Suite version 1.6.x, you need to change the redirect URL for the google application to https://<*ServicesPortalFQDN*>/wsp/wspconnect/connect/google after migrating the RealPresence CloudAXIS Suite to version 1.7.x.

Appendix 3: Cookies Used by the Applications

The RealPresence CloudAXIS Services Portal uses the following cookies:

- **WSP Application** Uses the userToken=0B8A4F41-AF5A-8809-6D34-F583AB7B5D06 and loginUser=admin cookies for requesting secure backend API calls.
- **userRole=ROLE_SUPER_ADMIN, ROLE_ADMIN, ROLE_USER** Based on the user role, the RealPresence CloudAXIS Services Portal shows different customized user interfaces. For example, only an Admin can see admin-related settings and other details.
- **i18next – en-US** i18Next library sets this cookie to handle Internalization for the WSP portal.

The RealPresence CloudAXIS Experience Portal uses the following cookies:

- **ManualLogin** This session cookie is a Boolean value used by the RealPresence CloudAXIS Experience Portal to determine if a login session was initiated by a user login or by an application integration or SSO.
- **DisplayName** This cookie is the name entered by a user when joining a meeting as an anonymous user, if the Remember Me function is enabled and the user checked the box during login. This cookie lasts for 14 days.
- **Address** This cookie is the e-mail address entered by a user when joining a meeting as an anonymous user, if the Remember Me function is enabled and the user checked the box during login. This cookie lasts for 14 days.
- **Tags** This cookie is reserved for future use.
- **SSOData** This cookie is a base64 encoded blob containing a session token and a username used to permit an enterprise user to re-login if the feature is enabled and the user checked the box at login. This cookie lasts for 14 days. Note that the session token expires independently as dictated by the rules of the system that issued it.

Appendix 4: DMA Factory Conference Settings Impact

The RealPresence DMA system uses conference templates and global conference settings to manage conference behavior. The following table shows the impact of the RealPresence DMA system's factory conference template settings on the RealPresence CloudAXIS Suite operations. For information on setting up a RealPresence DMA system conference template, see the *Polycom RealPresence DMA 7000 System Operations Guide*.

Conference Template Settings Impact

Feature	*Sub feature*	*Sub feature Description*	*Web Client Behavior*
General settings	Profile settings	Use existing profile	Not applicable
		RMX profile name	Works as documented
Conference settings	Conference mode		Both AVC and SVC are supported. If AVC only is selected, the RealPresence CloudAXIS web client operates in AVC (transcoded media) mode. If SVC only or Mixed AVC and SVC is selected, the RealPresence CloudAXIS web client operates in SVC (relayed media) or Mixed AVC and SVC mode.
	Cascade for bandwidth		Works as documented
	Video switching		Works as documented
	H.264 high profile		Works as documented
	Resolution		Works as documented
	Line rate		Fixed rate in web client
	Audio only		Not applicable
	Advanced settings	Encryption	Tied to the URL scheme: OFF for http, ON for https
		LRP	Works as documented
Video quality	People video definition	Video quality	Works as documented
		Max resolution	Works as documented

Feature	*Sub feature*	*Sub feature Description*	*Web Client Behavior*
		Video clarity	Works as documented
		Auto brightness	Works as documented
	Content video definition	Content settings	Works as documented
		Content protocol	Works as documented
Video settings	Presentation mode		Works as documented
	Send content to legacy endpoints		No Impact
	Same layout		Works as documented
	Lecture view switching		Works as documented
	Auto layout		Works as documented
	Layout		Works as documented
	Telepresence mode		Works as documented
	Telepresence layout mode		Works as documented
Audio settings	Echo suppression		Works as documented
	Keyboard noise suppression		Works as documented
	Audio clarity		Works as documented
Skins			Works as documented
Conference IVR	Override default service		Advanced—see the *Polycom RealPresence DMA 7000 System Operations Guide*
	Conference IVR service		May require use of DTMF pad in menu
	Conference requires chairperson		Users wait in the lobby until the chairperson joins the conference.
Recording	Record conference		Must be set to Immediately or Upon Request to enable recording

Feature	*Sub feature*	*Sub feature Description*	*Web Client Behavior*
	Recording link		Must be configured to enable recording
	Audio only		Works as documented.
	Indication of recording		Works as documented. Note: If enabled, a recording indication displays in both the video feed and in the web client GUI.