



ADMINISTRATOR GUIDE

Software 2.1.0 | May 2016 | 3725-03273-005F

Polycom® RealPresence® Web Suite



Copyright© 2016 , Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.



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

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

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

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

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

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

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

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

Contents

About This Guide	8
Audience, Purpose, and Required Skills	8
Terminology Used in this Guide	8
Get Help	9
Reference Documentation	9
Polycom® and Partner Resources	10
The Polycom® Community	10
Documentation Feedback	10
Product Overview	11
RealPresence Platform	12
About RealPresence Web Suite	13
RealPresence Web Suite Services Portal	14
RealPresence Web Suite Experience Portal	14
Standards Connector	14
Client Application	14
Users	14
Meetings	15
Social Media Contacts	15
Portal Deployment	15
Conferencing Modes	15
Ports and Protocols	17
Start and Restart Order for Components	20
Summary of Initial Setup Tasks	21
Activate Licenses	23
Activate Licenses within RealPresence Platform Director	23
Set Up Licensing for the RealPresence Web Suite Services Portal	23
Set Up Licensing for the RealPresence Web Suite Experience Portal	25
Allocate Licenses	27
View License Status	27

Activate Licenses for a Stand-Alone System	27
Activate the RealPresence Web Suite Experience Portal License Server Connection . . .	28
Activate Licenses in Online Mode	29
Activate Licenses in Offline Mode	30
Deactivate Licenses	32
Manage Certificates and Certificate Signing Requests	35
Generate Certificates and Certificate Signing Requests	35
View Certificates	38
Copy a CSR	38
Delete Certificates	39
Upload Certificates or a Certificate Chain	40
Configure Certificates for Reverse Proxy	42
RealPresence Web Suite Services Portal Server Settings	43
Set Web Addresses for the Portals	43
Select and Configure a User Authentication Mode	44
Set Up LDAP Authentication	44
Set Up Single Sign-On Authentication	45
Enable Email Notifications for Users	47
Configure Social Network Access	48
Enable Access to Google+ Contacts	48
Disable Access to Social Networking Contacts	49
Configure RealPresence DMA and Access Points	49
Add a RealPresence DMA System and Access Points	50
Edit a RealPresence DMA System Connection	53
Configure Conference Settings	54
Update the Language Pack for the RealPresence Web Suite Services Portal	56
Customize Email Templates	57
HTML Variables Used in Email Templates	58
Reset an Email Template	61
Customize and White Label the User Interface	61
Customize the User Interface	62
Change the Appearance of the Login Screen	63
Add a Notification Message for Users	63
Add a Logout URL	63
Change the User Interface Footer	64
Refresh the RealPresence Web Suite Experience Portal User Interface	64

RealPresence Web Suite Services Portal Platform Settings	66
Set the RealPresence Web Suite Services Portal Date and Time	66
Generate Certificates	67
Manage RealPresence Web Suite Services Portal Logging and Data Collection	67
Set the Log Level	68
Download Log Files	68
Enable Usage Data Collection	69
Enable SNMP Monitoring	70
Migrate the Application Data	70
Set Up License	70
Configure HTTP Forward Proxy Settings	70
Monitor the Environment with SNMP	72
SNMP Framework	72
Supported SNMP Versions	72
SNMP Notifications	73
Enable and Configure System Monitoring	74
User Management	77
Account Roles	77
Manage User Accounts	78
Required Internal System User Accounts	78
Change Your Password	79
Create User Accounts	79
Edit User Accounts	81
Delete User Accounts	82
Reset User Passwords	82
RealPresence Web Suite Experience Portal Conference Settings	83
Enable the RealPresence Web Suite Experience Portal for Conferencing	83
Configure the RealPresence Web Suite Experience Portal Conference Authentication Settings	84
Set Authentication Rules	85
Configure the RealPresence Web Suite Services Portal Authentication Agent	85
Configure the Resource Manager Authentication Agent	86
Configure the RealPresence Web Suite Experience Portal Conference Agents and Settings	88
Review Conference Lobby Rules	88
Configure the RealPresence DMA Agent	90
Configure the Conference Agent and Settings	90
Configure the WebRTC Agent	93
Update the Language Pack for the RealPresence Web Suite Experience Portal	94

Manage the RealPresence Web Suite Experience Portal User Roles	94
Default User Permissions	94
View and Change User Permissions	95
Role Assignment Rules	96
View and Change Roles Assignment Rules	96
RealPresence Web Suite Experience Portal Platform Settings	97
Set the RealPresence Web Suite Experience Portal Date and Time	97
Verify or Change the Network Configuration	98
Generate Certificate	98
Manage RealPresence Web Suite Experience Portal Logging	99
Set the Log Level	99
Download and View Log Files	100
Clear Log Files	101
Customize the User Interface	101
Import the Application Data	101
Activate License Information	101
Restart the RealPresence Web Suite Experience Portal Services or Server	101
Restart the RealPresence Web Suite Experience Portal Services	102
Reboot the RealPresence Web Suite Experience Portal Server	102
Enhanced Content	103
Configure the Enhanced Content Feature	103
Add Standards Connector Servers	105
Monitor Standards Connector Usage	106
RealPresence Web Suite Experience Portal Admin Management Menu	107
Manage RealPresence Web Suite Experience Portal Users	107
Change RealPresence Web Suite Experience Portal Administration Ports	108
Manage RealPresence Web Suite Experience Portal Administration Interface Certificates	109
Upgrading the Portals	111
Update RealPresence Web Suite Services Portal Software	111
Retrieve Current RealPresence Web Suite Services Portal Signed Certificate	111
Deploy a New RealPresence Web Suite Services Portal with Upgraded Software	111
Migrate Current Settings to the New RealPresence Web Suite Services Portal	112
Change the Network Settings of the New RealPresence Web Suite Services Portal	114
Update RealPresence Web Suite Experience Portal Software	115
Export Current RealPresence Web Suite Experience Portal Settings	115
Deploy a New RealPresence Web Suite Experience Portal with Upgraded Software	115
Import Settings to the New RealPresence Web Suite Experience Portal	116

Deploy New Standards Connector Servers for Enhanced Content	117
Restricted Shell Commands	118
Recommendations for Secure Access	122
Secure Web Access	122
Tunnel Access for Remote Users	122
Limitations Associated with Tunneling	123
Secure SIP Access for Guests	124
Edge Proxy Access for Guests	124
Additional Recommendations to Increase Security	125
Troubleshooting	126
Portal URL (FQDN) is unresponsive	127
RealPresence Web Suite Experience Portal fails to connect to RealPresence Web Suite Services Portal and get licensing information	127
User cannot create meetings	127
User cannot start a meeting using Meet Now function in RealPresence Web Suite Services Portal	127
User cannot launch the Welcome screen	128
Chrome user cannot join meeting with audio or video	128
Configured components do not respond	128
Super Admins and Admins cannot add Enterprise Directory users	128
User cannot send email notifications	128
User receives message: “Unable to create a conference with a personal VMR”	129
User receives message: “External server not set”	129
User receives message: “Resources are not available”	129
Enhanced Content users have trouble viewing shared content or see content updates only after long delays	129
Users of Enhanced Content cannot see content shared from standards-based endpoints or vice versa	129
WebRTC guest callers receive message: “No such VMR”	130
Remote WebRTC callers fail to connect or are disconnected when a mesh meeting is transitioned to a Multi-point Control Unit (MCU)	130
Administrator cannot download log files with Internet Explorer	130
User cannot see all participants in the Roster	130
Single Sign-On (SSO) is not working	130
SSO authentication has failed	131
Appendix 1: Deploy the WebRTC Solution	134
Overview of WebRTC	134
WebRTC versus SIP Plug-in	136

WebRTC Conference Modes	137
Polycom WebRTC Deployment Assumptions and Scenarios	138
Polycom WebRTC Solution Components	139
Required Solution Components	139
Optional Solution Components	140
Supported Operating Systems and Web Browsers	140
RealPresence Web Suite Pro	141
RealPresence DMA System	142
RealPresence Collaboration Server, Virtual Edition	142
RealPresence Access Director	143
Implementing the WebRTC Solution	143
Enable WebRTC Support in the RealPresence Access Director System	144
Enable WebRTC Support in the RealPresence Collaboration Server System	145
Enable WebRTC Support in the RealPresence DMA System	145
Enable WebRTC Support in the RealPresence Web Suite Pro System	147
Appendix 2: Set Up Enterprise Directory for Single Sign-On	150
Create a RealPresence Web Suite Services Portal User Account in Enterprise Directory ..	150
Set a Service Principal Name for the RealPresence Web Suite Services Portal User Account in Enterprise Directory	151
Generate a Keytab File for the RealPresence Web Suite Services Portal User	151
Appendix 3: Create an App to Access Google+ Social Media Contacts	153
Appendix 4: Cookies Used	155
Appendix 5: Conference Template Settings Impact	156
Appendix 6: Log Management	159
Additional Required Information for Debugging Issues	159
Server-side Logs	159
RealPresence Platform Component Logs	160
Capture RealPresence DMA Logs	160
Capture RealPresence Collaboration Server (RMX) Logs	161
Capture RealPresence Access Director Logs	162
Client-side Logs	163
Collect Primary Client Logs on Windows	163
Collect Primary Client Logs on Mac	163
Collecting MEA Server and WSP Client Logs	164
Web Client Console Logs	164
Enable Enhanced Log Level for Web Client Console Logs	164

Collect Enhanced Logs in the RealPresence Web Suite Services Portal	165
Enable Enhanced Logging on Google Chrome	165
Web Client Console Logs—Google Chrome	166
Web Client Console Logs—Mozilla Firefox	167
Web Client Console Logs—Internet Explorer	168

About This Guide

This guide describes how to configure and administer Polycom® RealPresence® Web Suite and RealPresence Web Suite Pro. It assumes that you have successfully deployed the two portals, completed the basic network configuration, and verified that you can log in to them, as described in the *Polycom RealPresence Web Suite Getting Started Guide* (available at [Polycom Support](#)).

Audience, Purpose, and Required Skills

This guide is written for the telecommunications administrator responsible for configuring, maintaining, and supporting the telecommunications infrastructure and video conferencing environment. It assumes the following knowledge and skills:

- Knowledge of current telecommunications practices, protocols, and principles.
- Experience implementing and maintaining telecommunication, video teleconferencing, and voice or data equipment.
- Familiarity with virtual machine environment, networking, security certificates, and software configuration.

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.

Term	Definition
Apache Tomcat	An open-source web server and application container that runs the RealPresence Web Suite Services Portal application.
Fully Qualified Domain Name (FQDN)	An example of an FQDN is dma.example.com.
Network Time Protocol Server (NTP)	An NTP server provides accurate time and date information for the devices configured to use it. For proper operation, the RealPresence Web Suite portals and the other components with which they communicate must have their time in sync, which is accomplished by having them all use the same NTP servers.
nginx	An HTTP server used to render static content and delegate requests to Apache Tomcat.
RealPresence Web Suite Experience Portal	The component of RealPresence Web Suite where users attend meetings. Also known as the Meeting Experience Application (MEA).

Term	Definition
RealPresence Web Suite Services Portal	The component of RealPresence Web Suite that handles scheduling meetings, adding users, and adding contacts. Also known as the Web Services Portal (WSP).
Virtual Edition	Indicates that a RealPresence Platform component is a software-based virtual machine.
Virtual Meeting Room (VMR)	A virtual meeting space that users and endpoints can join to participate in a multi-party video conference. VMRs are identified and addressed by numeric or alphanumeric IDs. A VMR may be personal or temporary. A personal VMR (also known as a persistent or static 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 <i>Polycom RealPresence DMA 7000 System Operations Guide</i> (available at Polycom Support) for more information on VMR management.
VMR prefix	Specifying a VMR prefix value allows the RealPresence Web Suite Services Portal and the RealPresence Web Suite Experience Portal to know where to direct requests concerning a specific 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.

Get Help

For more information about installing, configuring, and administering Polycom products, refer to Documents and Downloads at [Polycom Support](#).

Reference Documentation

In addition to this Administrator Guide, the following documentation is available on the [Polycom RealPresence Web Suite Support](#) site:

- *RealPresence Web Suite Release Notes*
- *RealPresence Web Suite Getting Started Guide*
- *RealPresence Web Suite Offer of Source for Open-Source Software*
- *RealPresence Web Suite User Guide*
- *RealPresence Web Suite Quick Tips Guide*

VMware® vSphere® support and documentation are available at:

- <https://www.VMware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html> (and select documentation for your respective version)
- <https://my.VMware.com/web/VMware>

Microsoft® Hyper-V® support and documentation are available at:

- <https://technet.microsoft.com/en-us/library/hh831531.aspx> (Hyper-V in Windows Server 2012 R2)
- <https://technet.microsoft.com/library/hh833684.aspx> (Hyper-V Server 2012 R2)

Polycom® and Partner Resources

To learn more about Polycom® RealPresence® Platform products, visit [Polycom Support](#) for links to information and downloads for the following.

- Polycom® RealPresence® DMA® 7000
- Polycom® RealPresence® Resource Manager
- Polycom® RealPresence® Access Director™
- Polycom® RealPresence® Collaboration Server
- Polycom® RealPresence® Platform Director

To find all Polycom partner solutions, see [Strategic Global Partner Solutions](#).

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.

Documentation Feedback

We strive to improve the quality of our documentation, and we appreciate your feedback. Please send your email with questions or suggestions to DocumentationFeedback@polycom.com.

Product Overview

Polycom® RealPresence® Web Suite enhances the Polycom® RealPresence® Platform by providing access using web browser to a shared meeting and collaboration experience that can include participants from the hosting organization and guests from outside the organization.

The RealPresence Web Suite Pro license enhances RealPresence Web Suite with support for the following:

Web Real-Time Communication (WebRTC) An HTML5-based communication technology that provides high-quality video and audio communications capabilities in WebRTC-capable browsers such as Google Chrome without requiring a plug-in. The RealPresence Platform WebRTC solution supports conferencing between WebRTC clients and other Polycom and third-party clients and endpoints.

For information about enabling WebRTC, see [Appendix 1: Deploy the WebRTC Solution](#).

Enhanced Content Uses the capabilities of HTML5 content sharing to provide far greater content and collaboration functionality, including multiple content streams, multiple participants sharing and annotating content concurrently, and the sharing of documents, whiteboards, and blackboards.

For information about enabling Enhanced Content, see [Enhanced Content](#).

Polycom® Concierge Polycom's solution that enables users to pair their personal devices (computer, tablet, or phone) running Polycom® RealPresence® Mobile or Polycom® RealPresence® Desktop directly to a Polycom® RealPresence® Group Series system. This enables users to wirelessly connect to the room system and join calendar events. The personal devices can be used to receive and share content and (depending on each user role, permissions, and personal device type) to access control functions such as recording, roster display, and chat.

For information about enabling the Polycom Concierge solution, see the *Polycom Concierge Deployment Guide*.

This guide covers RealPresence Web Suite both with and without the Pro license, and references to RealPresence Web Suite generally apply to both. RealPresence Web Suite Pro is specifically called out in the context of information related to the additional functionality provided by that license.

RealPresence Web Suite includes the following components described in the [About RealPresence Web Suite](#) section:

- RealPresence Web Suite Services Portal
- RealPresence Web Suite Experience Portal (includes RealPresence Web Suite Client)
- Standards Connector (RealPresence Web Suite Pro only)

This guide describes how to configure and manage the RealPresence Web Suite components.

This section is organized as follows:

- [RealPresence Platform](#)
- [About RealPresence Web Suite](#)
- [Ports and Protocols](#)
- [Start and Restart Order for Components](#)

RealPresence Platform

This section describes the RealPresence Platform of which RealPresence Web Suite and RealPresence Web Suite Pro are a part.

The RealPresence Platform product suite enables standards-based video conferencing and 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

Platform Component	Required or Optional	Purpose
Polycom® RealPresence® Distributed Media Application™ (DMA®), Virtual Edition	Required	Signaling, call control, and bridge virtualization
Polycom® RealPresence® Collaboration Server (RMX®), Virtual Edition	Required	Multi-point Control Unit (MCU), or bridge, for hosting conferences
Polycom® RealPresence® Resource Manager	Optional	Provisioning and managing endpoints
Polycom® RealPresence® Access Director™ solution*	Optional	Network Address Translation (NAT)/firewall traversal
Polycom® RealPresence® Platform Director™	Optional	Licensing and monitoring component instances
Polycom® RSS™ recording and streaming server	Optional	Media recording
Polycom® RealPresence® Media Suite (formerly Polycom® RealPresence® Capture Server)	Optional	Media recording
*An Acme Packet Net-Net Enterprise Session Director may also be used to secure firewall traversal.		



Caution: Disable incompatible “Secure Conference” feature on MCUs

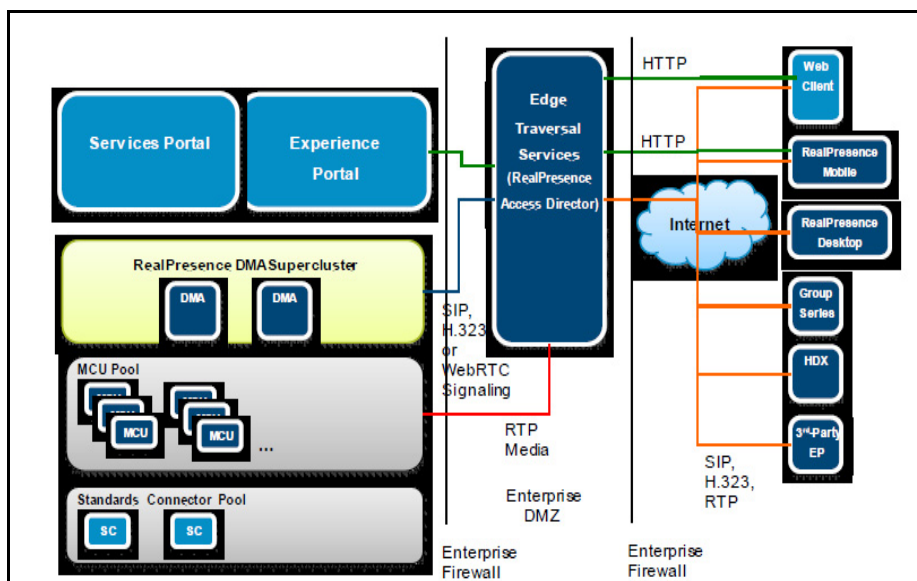
By default, RealPresence Collaboration Server MCUs support a “secured” conference mode. When a chairperson selects it, the MCU fails to communicate that status change or any subsequent information about the conference to the RealPresence DMA system managing it (or to any other entity). RealPresence Web Suite relies on the RealPresence DMA system for conference information. Since neither entity is aware that the conference is locked, the conference roster, chat, and content are not secured.

Polycom strongly recommends disabling the “Secure Conference” feature on MCUs managed as conferencing resources by a RealPresence DMA system. You can do so by deleting the Dual-tone Multi-frequency (DTMF) commands that control it (*71 and #71) on the DTMF Codes tab of the Conference Interactive Voice Response (IVR) Service Properties dialog box.

Conferences can be locked using the RealPresence DMA system Representational State Transfer Application Programming Interface (REST API), and that method of securing a conference is fully compatible with RealPresence Web Suite.

The following diagram shows the components in a typical RealPresence Platform solution.

Polycom RealPresence Platform Components



RealPresence Platform components work with the RealPresence Web Suite system 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 RealPresence Mobile application.

If Polycom RSS or RealPresence Media Suite (formerly RealPresence 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.

About RealPresence Web Suite

This section describes RealPresence Web Suite and its components. Meetings are scheduled in the RealPresence Web Suite Services Portal and attended through the RealPresence Web Suite Experience Portal. Participating in meetings requires access only to the RealPresence Web Suite Experience Portal

using an HTML5-compliant browser or downloaded plug-in and a URL link sent in an email or instant message.

RealPresence Web Suite Services Portal

Through the RealPresence Web Suite Services Portal, users create and initiate online video conference meetings. Scheduling a meeting in the RealPresence Web Suite Services Portal requires user or administrator account access (see [Account Roles](#)).

Users create meetings by logging in to the RealPresence Web Suite Services Portal, selecting the type of meeting they want to create, setting the meeting parameters, and entering a list of participants to invite. In the administration interface of the RealPresence Web Suite Services Portal, administrators can create and manage users and configure many aspects of the RealPresence Web Suite system.

RealPresence Web Suite Experience Portal

In the RealPresence Web Suite Experience Portal, users attend meetings and interact with features such as content sharing and group chat. In the administration interface of the RealPresence Web Suite Experience Portal, administrators configure key aspects of the RealPresence Web Suite system, including conference and authentication configuration and, for RealPresence Web Suite Pro, WebRTC support and Enhanced Content.

Standards Connector

One or more Standards Connector servers are required to support the Enhanced Content feature of RealPresence Web Suite Pro. The Standards Connector provides transcoding of the HTML5 data distributed by the RealPresence Web Suite Experience Portal into H.264 video streams signaled through Session Initiation Protocol (SIP) and Binary Floor Control Protocol (BFCP) and distributed by an MCU. This makes it possible to share content between HTML5 clients and standards-based clients.

Client Application

Users connect to a RealPresence Web Suite conference using their web browser as the client application. For non-WebRTC conferences and browsers, RealPresence Web Suite offers to download the Polycom RealPresence Media Framework Client (MFW) plug-in that enables SIP.

If RealPresence Web Suite has the Pro license and the other requirements for supporting WebRTC are met, a WebRTC-capable browser can use WebRTC to initiate or join a conference. The RealPresence Web Suite Experience Portal provides the Javascript and HTML5 that establishes the Real-Time Communication (RTC) session. No plug-in is needed.

Users

You can add users to the RealPresence Web Suite Services Portal locally or by integrating with an enterprise Lightweight Directory Access Protocol (LDAP) server (Microsoft® Active Directory® is supported). With LDAP integration enabled, enterprise users can use their domain network credentials to schedule and start meetings in the RealPresence Web Suite Services Portal and attend meetings in the RealPresence Web Suite Experience Portal.

Meetings

Users log in to the RealPresence Web Suite Services Portal, select the **Schedule Meeting** option, choose meeting options, select the participants they want to invite, and then schedule a meeting.

The configured Simple Mail Transfer Protocol (SMTP) server sends the email notifications to each invited participant. The invitation includes a URL link to the meeting and can include information for how to access meetings using SIP, H.323, Integrated Services Digital Network (ISDN), Tunneling, or Public Switched Telephone Network (PSTN).

The RealPresence Web Suite Services Portal contacts the RealPresence DMA system to create a VMR using the configured conference template. The audio and video communication portions of most meetings are hosted on and facilitated by a MCU, or bridge (the RealPresence Collaboration Server).

If WebRTC mesh mode is enabled under RealPresence Web Suite Pro, a meeting that is composed of a small number of WebRTC participants can take place in mesh mode, where the audio and video media are exchanged directly between the clients without using any MCU resources.

When a bridge-based meeting takes place, the RealPresence DMA system validates the VMR and routes the call to a RealPresence Collaboration Server MCU so that participants can exchange audio and video.

In the RealPresence Web Suite Services Portal, users can also start a meeting immediately (an ad hoc meeting). In that case, they are transferred to an RealPresence Web Suite Experience Portal session and prompted to begin inviting participants.

Social Media Contacts

If the RealPresence Web Suite Services Portal administrator creates an app to access Google+™ social media contacts and enables access to Google+ contacts in the RealPresence Web Suite Services Portal, users can invite participants to meetings from an aggregated list of the meeting creator's Google+ contacts.

When users select social media contacts in the RealPresence Web Suite Services Portal, a URL is sent to the contacts on that social messaging service. The invited participants can click the URL or paste it into their browser to join the meeting.

Portal Deployment

The RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal are each packaged in Open Virtualization Archive (OVA) files that can be deployed on VMware® ESXi hosts or in a VMware vCenter. Both portals are also packaged in Hyper-V® Export (*.zip) files that can be deployed on Microsoft® Hyper-V servers. The Standards Connector runs on the same software as the RealPresence Web Suite Experience Portal, only configured differently, so the same file is used to deploy it.

The environment into which the RealPresence Web Suite portals are deployed must meet the requirements outlined in the Release Notes for the version you are deploying.

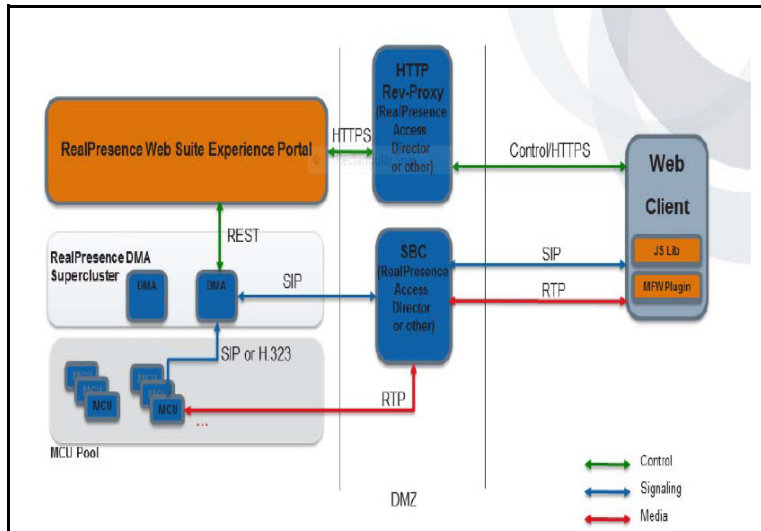
Conferencing Modes

The following sections describe and illustrate three conferencing modes. The first is available in all RealPresence Web Suite configurations. The second and third modes support WebRTC and require the RealPresence Web Suite Pro license and the proper configuration of all components in the RealPresence Platform environment.

Standards-based Conference Mode

RealPresence Web Suite supports standard SIP conferencing, as shown in the following diagram. Web applications (browsers) require a plug-in to join the conference.

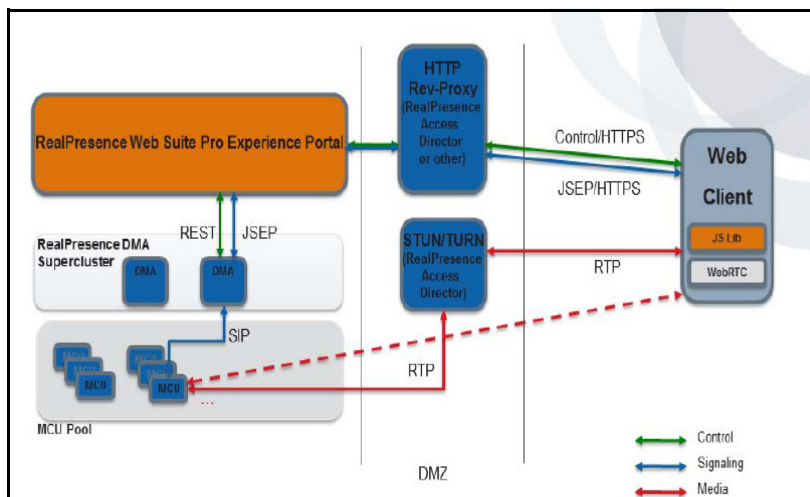
RealPresence Web Suite: SIP Call to MCU



Transcoded Conference Mode

Transcoded (or bridge) conferences are hosted on the RealPresence Collaboration Server, Virtual Edition, a WebRTC-enabled MCU. This lets WebRTC-enabled browsers connect to any conference with any type of participants. The following diagram shows a WebRTC call to a WebRTC-enabled MCU.

RealPresence Web Suite Pro: WebRTC Call to MCU



Mesh Conference Mode

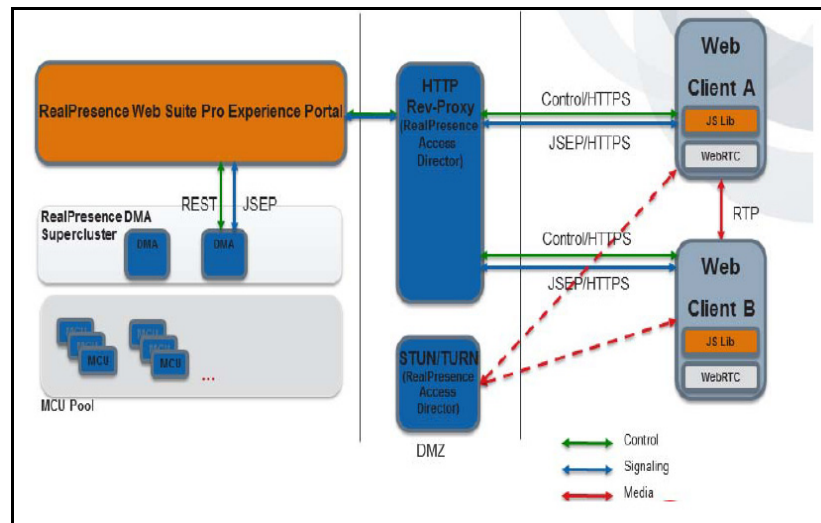
Mesh conference mode enables each WebRTC-enabled client application (browser) to send media directly to the other client applications in conference, rather than to an MCU. This allows greater capacity as minimal server-side resources are required for small conferences that include only WebRTC clients. An essential

However, mesh conferencing has the following limitations:

- Conference participants can only connect to a mesh conference using a WebRTC-enabled browser.

- The following diagram shows two WebRTC endpoints in a mesh conference.

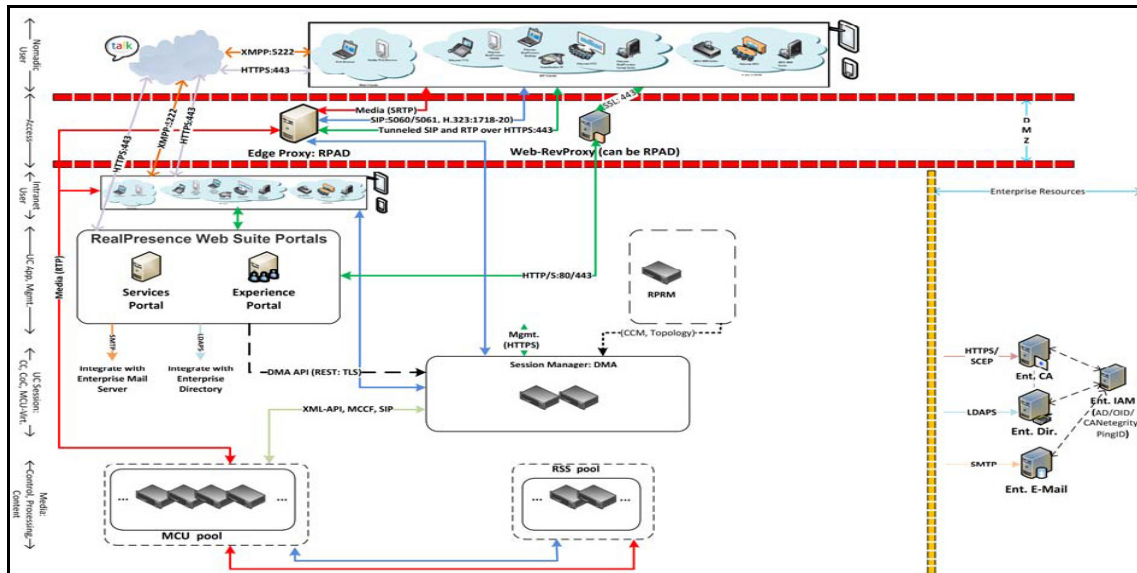
RealPresence Web Suite Pro: WebRTC Mesh Calls



This section illustrates and describes the ports and protocols used by the RealPresence Web Suite portals.

The following graphic shows how various ports and communications protocols interact in a sample

Ports and Protocols used in a typical RealPresence Web Suite Deployment



The following table describes the inbound and outbound ports and protocols that handle communications between the portals and other RealPresence system components and network elements.

Inbound and Outbound Protocols and Ports

Protocol/Function	Communication	Ports
HTTP/HTTPS	From web clients to the RealPresence Web Suite Services and Experience Portals.	Transmission Control Protocol (TCP) 443. Port 80 is also enabled, but it redirects to 443. Provides web browser access to the User Interface (UI) and REST APIs.
HTTPS	Between the RealPresence Web Suite Experience Portal and the RealPresence DMA system.	TCP 8443 from RealPresence Web Suite Experience Portal to RealPresence DMA system. TCP 9443 from RealPresence DMA system to RealPresence Web Suite Experience Portal.
HTTPS	Access to RealPresence Web Suite Experience Portal administration interface.	TCP 9445.
HTTPS	Enhanced content sharing service.	TCP 9081/9981.
HTTPS (Tunneling)	From web clients to RealPresence Access Director (version 3.1 is required to set up tunneling in a RealPresence Web Suite environment).	TCP 443. Port 80 is also enabled, but it redirects to 443. Media streams are communicated through RealPresence Access Director.
Secure Shell (SSH)	For SSH access to restricted shell.	TCP 22.
Network Time Protocol (NTP)	Between the portals and an NTP server.	User Datagram Protocol (UDP) 123

Inbound and Outbound Protocols and Ports

Protocol/Function	Communication	Ports
Dynamic Host Configuration Protocol (DHCP)	Between the portals and a DHCP server.	UDP 67/68.
SMTP	Between the RealPresence Web Suite Services Portal and the SMTP server.	TCP 25 for non-secure (SMTP). TCP 587/465 for secure (SMTP-S).
Simple Network Management Protocol (SNMP)	Between SNMP agents and managers.	UDP 161/162.
LDAP	Between the RealPresence Web Suite Services Portal and the 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 Web Suite Services Portal uses this port to communicate with social networking apps to get contact presence information and deliver instant message invitations.
SIP	Between client endpoints and the RealPresence DMA system or intermediate edge proxy (RealPresence Access Director or Acme).	5060 (UDP/TCP)/5061 (TLS). 443 (TCP) for HTTPS Tunneling. SIP is the signaling protocol used by the RealPresence Web Suite plug-in web client, RealPresence Mobile, and other SIP endpoints.
Real-time Transport Protocol (RTP) Real-time Control Protocol (RTCP) Secure Real-time Transport Protocol (SRTP) Secure Real-time Control Protocol (SRTCP)	Between client endpoints (mesh conference) or between endpoints and MCU or intermediate edge proxy (RealPresence Access Director or Acme).	RealPresence Web 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 video and audio media between web-based clients and the MCU. RTCP and SRTCP provide out-of-band statistics and control information for an associated RTP or SRTP flow.

Inbound and Outbound Protocols and Ports

Protocol/Function	Communication	Ports
Binary Floor Control Protocol (BFCP)	Between client endpoints and MCU or intermediate edge proxy (RealPresence Access Director or Acme).	3238 (UDP/TCP). BFCP is the signaling protocol used by SIP clients to negotiate content sharing.
Enhanced Content Sharing (WebSocket)	Between Content Sharing Agent (on RealPresence Web Suite Experience Portal) and Content Sharing Manager (on RealPresence Web Suite Experience Portal or Standards Connector server).	TCP 9332/9335. If the RealPresence Web Suite Experience Portal built-in Standards Connector function is being used (no dedicated Standards Connector server), port 9335 must be open only for localhost.

Start and Restart Order for Components

When you start RealPresence Web Suite, be sure to start the RealPresence Web Suite Services Portal and the configured RealPresence DMA system before starting the RealPresence Web Suite Experience Portal. Failure to do so impacts the API that handles feature functionality on the RealPresence Web Suite Experience Portal.

When you restart the RealPresence Web Suite Services Portal or the configured RealPresence DMA system, be sure to also restart the RealPresence Web Suite Experience Portal afterwards (see [Customize the User Interface](#)). Failure to do so impacts the API that handles feature functionality on the RealPresence Web Suite Experience Portal.

Summary of Initial Setup Tasks

This section briefly describes the configuration tasks required to complete the implementation of a new Polycom® RealPresence® Web Suite system. This section includes detailed descriptions and procedures that are to be read first to get an overview of the process.

This section assumes that you have deployed the two portals, completed the basic network configuration, and verified that you can log in to each portal, as described in the *Polycom RealPresence Web Suite Getting Started Guide* (available at [Polycom Support](#)).



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

All configuration steps on both the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal must be completed by a user with Super Admin credentials. If you have not done so already, log in to each portal for the first time using `admin` as the user name and `Polycom12#$` as the password. At a minimum, you must change that password. For greater security, add individual administrator accounts for each authorized person and delete the generic admin account.

For information on the account roles, see [Account Roles](#).

Complete the following tasks to set up a new RealPresence Web Suite system. Because the RealPresence Web Suite Services Portal includes some of the configuration steps for both portals, its configuration tasks must be completed first as per the following list.

Set Web Addresses for the Portals In the RealPresence Web Suite Services Portal, specify the URL for accessing each portal. Note that the portals must always be accessed by their Fully Qualified Domain Name (FQDN), not IP address.

Set Secure Passwords for the Required Internal System User Accounts

Change the default passwords for the internal system user accounts as soon as possible for security reasons. You will need to specify these passwords in the RealPresence Web Suite Experience Portal later when performing the related configuration tasks.

Set the RealPresence Web Suite Services Portal Date and Time If you did this using console access after deployment, verify the time settings in the RealPresence Web Suite Services Portal administration interface. If not, set the time zone and Network Time Protocol (NTP) servers now.

Activate Licenses How you activate licenses depends on whether your system is deployed stand-alone or within RealPresence Platform Director.

Obtain and Install CA-signed Certificates for Both Portals Polycom strongly recommends installing certificates signed by a commercial Certificate Authority (CA) in all components of the RealPresence Platform solution, including the RealPresence Web Suite portals.

Configure RealPresence DMA and Access Points In the RealPresence Web Suite Services Portal, specify the RealPresence DMA system to use for RealPresence Web Suite meetings and the access points for connecting to that system. Meeting participants connect to their conference through an access point (generally a network location connected directly to the RealPresence DMA system or indirectly through the RealPresence Access Director system).

Select and Configure a User Authentication Mode The RealPresence Web Suite Services Portal handles authentication for users. You can configure a connection to your organizational Lightweight Directory Access Protocol (LDAP) server (Microsoft® Active Directory® is supported) for authenticating user credentials. You can also configure the RealPresence Web Suite Services Portal to support Single Sign-On (SSO) so that users logged in to the domain do not need to re-enter their Enterprise Directory credentials.

Manage User Accounts The RealPresence Web Suite Services Portal manages all user accounts (except for the RealPresence Web Suite Experience Portal Super Admin), including the internal system users. For security reasons, you must change the default passwords of those system users. You must also create individual accounts for authorized administrators and delete the default *admin* account. Connecting the RealPresence Web Suite Services Portal to Enterprise Directory enables all the Enterprise Directory members to create, manage, and attend meetings. There is no need to add them manually in RealPresence Web Suite. You can, however, add an Enterprise Directory user manually in order to change the user role or to disable or enable the user in RealPresence Web Suite.

Enable Email Notifications for Users The RealPresence Web Suite Services Portal must be able to send email invitations to meetings and other notifications to users. To enable it to do so, configure the connection to your organizational Simple Mail Transfer Protocol (SMTP) server.

Enable and Configure System Monitoring Configure Simple Network Management Protocol (SNMP) on the RealPresence Web Suite Services Portal to enable it to communicate data about both the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal servers to the RealPresence Platform Director system or another SNMP manager.

Set the RealPresence Web Suite Experience Portal Date and Time If you did this using console access after deployment, verify the time settings in the RealPresence Web Suite Experience Portal administration interface. If not, set the time zone and NTP servers now.

Enable the RealPresence Web Suite Experience Portal for Conferencing In the RealPresence Web Suite Experience Portal, enable it and specify its external web addresses (used by human users) and internal web addresses (used by the internal system users for inter-portal communications).

Configure the RealPresence Web Suite Experience Portal Conference Authentication Settings

The RealPresence Web Suite Experience Portal authenticates users with the RealPresence Web Suite Services Portal to enable them to host or attend meetings. You must configure the rules used for authentication and the authentication agent that queries the RealPresence Web Suite Services Portal (this is the internal system user *meaauth*).

Configure the RealPresence Web Suite Experience Portal Conference Agents and Settings In order for the RealPresence Web Suite Experience Portal to host meetings, you must configure the agent that queries the RealPresence Web Suite Services Portal for meeting information (this is the internal system user *meaconf*) and the agent that queries the RealPresence DMA system to manage and obtain meeting rosters and control conference recording. You must also configure the same access points in the RealPresence Web Suite Experience Portal that you defined in the RealPresence Web Suite Services Portal for connecting to the RealPresence DMA system.

Manage the RealPresence Web Suite Experience Portal User Roles The RealPresence Web Suite Experience Portal assigns meeting attendees one of three roles (Chairperson, Participant, or Guest), which have different permissions in the meeting. You can review and modify, if desired, the permissions granted to each role and the rules that determine which role is assigned to a caller.

Activate Licenses

How you manage licenses in the Polycom® RealPresence® Web Suite system depends upon whether you are operating your RealPresence Web Suite system in stand-alone mode or within a RealPresence Platform Director solution.

Follow one of these licensing procedures to license your RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal.

- [Activate Licenses within RealPresence Platform Director](#)
- [Activate Licenses for a Stand-Alone System](#)

Activate Licenses within RealPresence Platform Director

When you deploy a RealPresence Web Suite system within a RealPresence Platform Director solution, you must manage licensing through RealPresence Platform Director for both portals. This involves the following tasks:

- [Set Up Licensing for the RealPresence Web Suite Services Portal](#)
- [Set Up Licensing for the RealPresence Web Suite Experience Portal](#)
- [Allocate Licenses](#)
- [View License Status](#)



Note: Reboot RealPresence Platform Director if necessary

If license changes have been made to the Polycom Licensing Center (such as adding a new type of license), RealPresence Platform Director must be rebooted in order to pick up those changes.

Set Up Licensing for the RealPresence Web Suite Services Portal

First, if you did not create the RealPresence Web Suite Services Portal instance within the RealPresence Platform Director system, you need to add it to that system. When you create or add the RealPresence Web Suite Services Portal within a RealPresence Platform Director system, the RealPresence Web Suite Services Portal automatically connects to the RealPresence Platform Director licensing server.



Note: Log out of the RealPresence Web Suite Services Portal first

Log out of the RealPresence Web Suite Services Portal before adding it to RealPresence Platform Director.

See the *Polycom RealPresence Platform Director Administrator Guide* (available at [Polycom Support](#)) for further information about licensing RealPresence Web Suite within that platform.



Note: Licensing for existing RealPresence Web Suite Services Portal instances

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

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

- 1 In the RealPresence Platform Director system, create or add the RealPresence Web Suite Services Portal instance as per the instructions in the *RealPresence Platform Director Administrator Guide*.
- 2 Log in to the RealPresence Web Suite Services Portal and if you have not already done so, change the administrator password and accept the licensing agreement.
- 3 Navigate to the RealPresence Web Suite Services Portal settings in RealPresence Platform Director and change the password to match that on the RealPresence Web Suite Services Portal instance. Passwords in both places must match in order for the RealPresence Platform Director system to properly manage licensing for RealPresence Web Suite instances.
- 4 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > License**.
- 5 Verify the following license settings as shown next:
 - The IP address for the Licensing Server is the IP address of the Platform Director instance that manages the RealPresence Web Suite Services Portal.
 - The RealPresence Web Suite Services Portal License Information reflects an activated license.
 - The RealPresence Web Suite Experience Portal license is listed as not yet registered.

PLATFORM

DATE TIME CERTIFICATE LOGS MIGRATE **LICENSE** PROXY

Licensing Server

Server Address: 10.47.12.130 Refresh Connection
 Port: 3333

License Information

RealPresence® Web Suite Service Portal
 Version: 1.6.0.843-154212
 Device ID: 4204CC27-2844-CFAC-EA42-EE1F13AB3E1C
 Status: **ACTIVATED**

RealPresence® Web Suite Experience Portal
 -NOT YET REGISTERED-

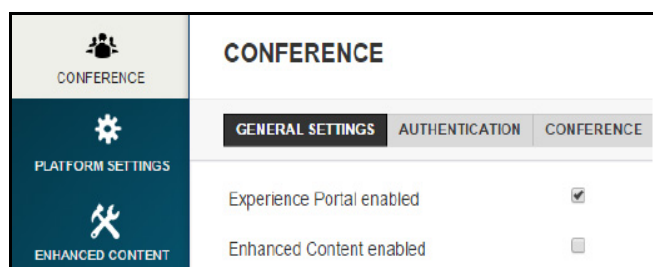
- 6 If the Server Address is incorrect or the RealPresence Web Suite Services Portal does not show ACTIVATED as the status, click **Refresh Connection**.
- 7 Continue to the next section for instructions on setting up licensing for the RealPresence Web Suite Experience Portal.

Set Up Licensing for the RealPresence Web Suite Experience Portal

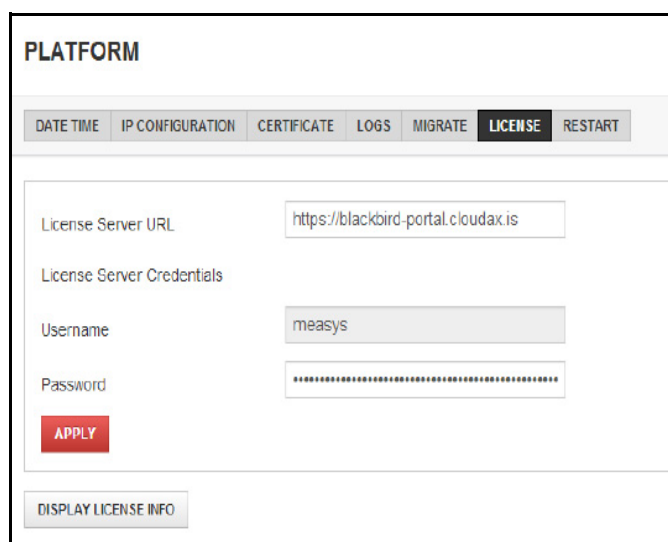
After the RealPresence Web Suite Services Portal license is activated, you can direct the RealPresence Web Suite Experience Portal to the RealPresence Web Suite Services Portal to obtain licensing.

To set up licensing for the RealPresence Web Suite Experience Portal:

- 1 In the RealPresence Platform Director system, create or add the RealPresence Web Suite Experience Portal instance per the instructions in the *RealPresence Platform Director Administrator Guide* (available at [Polycom Support](#)).
- 2 Log in to the administration interface for the RealPresence Web Suite Experience Portal by using its Fully Qualified Domain Name (FQDN) and port number 9445.
For example, type `https://<experienceportal.domain.com>:9445`.
- 3 If you have not already done so, change the administrator password and accept the licensing agreement.
- 4 Navigate to **Conference > General Settings**.
- 5 Select **RealPresence Web Suite Experience Portal enabled**, as shown next.



- 6 Navigate to **Platform Settings > License**.
- 7 In the **License Server URL** field, enter the URL of the RealPresence Web Suite Services Portal used to retrieve the licensing information as shown next.



- 8 Under **License Server Credentials**, enter the correct password for the *measys* system user.
The default password is *measys*, which must be changed for security reasons. See [Required Internal System User Accounts](#).
- 9 Click **Apply**.
- 10 Navigate to **Platform Settings > Restart > Reboot Server**.
Rebooting the server associates the RealPresence Web Suite Experience Portal with the RealPresence Web Suite Services Portal and enables the RealPresence Web Suite Experience Portal to pick up licensing information from the RealPresence Web Suite Services Portal.
- 11 After the RealPresence Web Suite Experience Portal server reboots, log in to the RealPresence Web Suite Services Portal as a Super Admin and navigate to **Platform Settings > License**.
- 12 Verify the following license settings on the RealPresence Web Suite Services Portal:
 - The IP address for the Licensing Server must be the IP address for the RealPresence Platform Director instance that manages this RealPresence Web Suite Services Portal.
 - The RealPresence Web Suite Services Portal License Information section indicates an activated license.
 - The RealPresence Web Suite Experience Portal section indicates an activated license.
 If the RealPresence Web Suite Experience Portal failed to become licensed, see the troubleshooting topic [RealPresence Web Suite Experience Portal fails to connect to RealPresence Web Suite Services Portal and get licensing information](#).

While deploying RealPresence Web Suite, it is necessary for the RealPresence Web Suite Experience Portal to be able to establish a connection with the RealPresence Web Suite Services Portal to obtain licensing information.

The following are the minimum requirements for the licenses to be applied.

- Each server must be able to resolve the FQDN of the other server.
- In the MEA configuration, perform the following steps including defining of WSP:
 - 1 Select **Conference > Authentication > Service Portal Configuration**. Add the WSP FQDN as the Target URL and enter the meaauth password.
 - 2 Select **Conference > Conference > Service Portal Conference**. Add the WSP FQDN as the Target URL and enter the meaconf password.
 - 3 Select **Conference > Conference > DMA**. Define the DMA to save the conference settings.
 - 4 Select **Platform Settings > License**. Add the WSP FQDN as the License Server URL and enter the measys password.

Once the settings are saved and MEA is rebooted, the license page appears on WSP allowing license codes to be applied (in standalone deployments) or allowing MEA to be licensed using RealPresence Platform Director (in RealPresence One deployments).



Note: Additional configurations are required to get the solution fully up and running

These are the minimum requirements to allow the licenses to be applied. Also, there are additional configurations required to get the solution fully up and running.

Next, you can allocate count-based licenses to the RealPresence Web Suite portals.

Allocate Licenses

The *RealPresence Platform Director Administrator Guide* provides instructions on allocating “Counted Feature” licenses for your RealPresence Web Suite (base licenses are allocated automatically). For RealPresence Web Suite, the count-based license is the number of Max Calls for the RealPresence Web Suite Experience Portal (shown as MEA-ATTENDEES in the RealPresence Web Suite Experience Portal). This represents the number of users who can attend meetings concurrently through this instance of the portal.

View License Status

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

To view license status in the RealPresence Web Suite Services Portal:

- » In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > License**.

To view license status in the RealPresence Web Suite Experience Portal:

- » In the RealPresence Web Suite Experience Portal administration interface, navigate to **Platform Settings > License > Display License Info**.

The RealPresence Web Suite Experience Portal retrieves licensing information from the RealPresence Web Suite Services Portal, which retrieves it from the Platform Director instance, so license updates can take up to an hour to appear on the RealPresence Web Suite Experience Portal.

Activate Licenses for a Stand-Alone System

If the RealPresence® Web Suite system operates in stand-alone mode (not managed by RealPresence® Platform Director), you have to activate licenses through the RealPresence Web Suite Services Portal for both the RealPresence Web Suite Experience Portal and the RealPresence Web Suite Services Portal. The RealPresence Web Suite Services Portal license is the RealPresence Web Suite product license.



Note: Stand-alone RealPresence Web Suite has a trial license

A RealPresence Web Suite system deployed outside of a RealPresence Platform Director solution is pre-configured with a 30-day trial license of RealPresence Web Suite Pro.

You can activate licenses in one of the following modes:

Online mode License information is sent directly to the Polycom Licensing Center for activation. The RealPresence Web Suite Services Portal must have Internet access to complete the activation.

Offline mode A file is prepared and sent to Polycom so that the Polycom Licensing Center can activate the license and send back an activation file.

Make sure you have the activation keys available when you begin activating the portal licenses. The activation keys are sent to you in an email after your company purchased RealPresence Web Suite.

Activate the RealPresence Web Suite Experience Portal License Server Connection

The RealPresence Web Suite Services Portal is the license server for the RealPresence Web Suite Experience Portal. Before you activate the RealPresence Web Suite Experience Portal licenses, activate the connection between the RealPresence Web Suite Experience Portal and the RealPresence Web Suite Services Portal.

To activate the RealPresence Web Suite Experience Portal connection to the RealPresence Web Suite Services Portal:

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > License**.
- 3 In the **License Server URL** field, enter the URL of the RealPresence Web Suite Services Portal used to procure your licensing information, as shown next.

PLATFORM

DATE TIME IP CONFIGURATION CERTIFICATE LOGS MIGRATE **LICENSE** RESTART

License Server URL

License Server Credentials

Username

Password

APPLY

DISPLAY LICENSE INFO

- 4 Under **License Server Credentials**, enter the correct password for the *measys* system user.
The default password is *measys*, which must be changed for security reasons. See [Required Internal System User Accounts](#).
- 5 Click **Apply**.
- 6 Navigate to **Platform Settings > Restart** and click **Reboot Server**.
Rebooting the server associates the RealPresence Web Suite Experience Portal with the RealPresence Web Suite Services Portal and enables the RealPresence Web Suite Experience Portal to pick up licensing information from the RealPresence Web Suite Services Portal. For more information to be able to establish a connection with the RealPresence Web Suite Services Portal and to obtain the licensing information, see [Set Up Licensing for the RealPresence Web Suite Experience Portal](#).

Once the RealPresence Web Suite Experience Portal license server connection is established, you can activate licenses for both portals. This is done in the RealPresence Web Suite Services Portal. Follow one of the following procedures, depending on whether the RealPresence Web Suite Services Portal has Internet access:

- [Activate Licenses in Online Mode](#)
- [Activate Licenses in Offline Mode](#)

After activating licenses, you may want to view license information in the RealPresence Web Suite Experience Portal to verify that it is properly licensed.

To view the license information in the RealPresence Web Suite Experience Portal:

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > License** and click **Display License Info**.

If the RealPresence Web Suite Experience Portal fails to be licensed, see the troubleshooting topic [RealPresence Web Suite Experience Portal fails to connect to RealPresence Web Suite Services Portal and get licensing information](#).

Activate Licenses in Online Mode

Activating licenses in online mode requires Internet access to communicate directly with the Polycom Licensing Center.

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

- 1 Log in to the RealPresence Web Suite Services Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > License**.

The License page displays license information for the RealPresence Web Suite Services Portal and the RealPresence Web Suite Experience Portal as shown next.

PLATFORM

DATE TIME
CERTIFICATE
DIAGNOSTICS
SNMP
MIGRATE
LICENSE
PROXY

Service Portal | Version 2.1.0.884-204071

Device ID: 421F891D-6114-F779-8F53-8E5162B33C74

Activation Mode: Online

Service Portal
Trial Version expires in next 29 days.

Enter Activation Key

Experience Portal | Version 2.1.0.9886587

Device ID: 431F89ED-9114-G779-9F53-1E5162B33C74

Activation Mode: Online

Experience Portal
Trial Version expires in next 29 days.

Enter Activation Key

Enhanced Content
Trial Version expires in next 29 days.

Enter Activation Key

Concurrent Users - 50 Users
+

Enter Activation Key
Count

3 Enter your activation keys as follows:

- In the **RealPresence Web Suite Services Portal** field, enter the key labeled SERVICE PORTAL.
- In the **RealPresence Web Suite Experience Portal** field, enter the key labeled RealPresence Web Suite Experience Portal.
- For RealPresence Web Suite Pro, in the **Enhanced Content** field, enter the key labeled Enhanced Content Feature.
- Under **Concurrent Users**, enter a concurrent user license activation key (labeled 150 SESS LIC, 100 SESS LIC, or 50 SESS LIC) and in the adjacent count field, the number of such licenses to apply. If you have other concurrent user license activation keys to enter, click the + button to add another set of activation key and count fields.

For instance, to enable 350 concurrent users, you could enter a 150 SESS LIC license key and set its count at 2, and then click the + button, enter a 50 SESS LIC key, and set its count at 1.

4 Click **ACTIVATE**.

The screen refreshes, a message indicates the license activation was successful, and a list of activated licenses is displayed.

Activate Licenses in Offline Mode

You can activate licenses for the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal in offline mode. To do so, perform the following procedure twice. First, complete the procedure to activate the license for the RealPresence Web Suite Services Portal. Then, repeat the procedure to activate licenses for the RealPresence Web Suite Experience Portal.



Caution: The RealPresence Web Suite Experience Portal license server connection must be activated first

The RealPresence Web Suite Services Portal is the license server for the RealPresence Web Suite Experience Portal. Activate the RealPresence Web Suite Experience Portal license server connection before activating RealPresence Web Suite Experience Portal licenses on the RealPresence Web Suite Services Portal. See [Activate the RealPresence Web Suite Experience Portal License Server Connection](#).

To activate RealPresence Web Suite Services Portal or RealPresence Web Suite Experience Portal licenses in offline mode:

- 1 In the RealPresence Web Suite Services Portal, navigate to **Platform Settings > License**.
- 2 For the portal you are activating, set **Activation Mode** to **Offline**.
- 3 For the portal you are activating, enter the activation keys in the appropriate fields on the right:
 - The first time you perform this procedure, enter the activation key for the RealPresence Web Suite Services Portal (labeled Service Portal).
 - The second time you perform this procedure, enter the following:
 - ◆ RealPresence Web Suite Experience Portal key (labeled RealPresence Web Suite Experience Portal)
 - ◆ Enhanced Content key (RealPresence Web Suite Pro only; labeled Enhanced Content Feature)
 - ◆ Concurrent user license activation key (labeled 150 SESS LIC, 100 SESS LIC, or 50 SESS LIC) and in the adjacent count field, the number of such licenses to apply. If you have additional concurrent user license activation keys to enter, click the **+** button to add another set of activation key and count fields.

For instance, to enable 350 concurrent users, enter a 150 SESS LIC license key and set its count at 2, and then click the **+** button, enter a 50 SESS LIC key, and set its count at 1.
- 4 For the portal you are activating, click **Download**.
The activation request is a .bin file that is downloaded to the computer.
- 5 Log in to the [Polycom Licensing Center](#) with your credentials.
- 6 In the left menu, click **Upload Capability Request**.
- 7 On the Upload Capability Request page, click **Browse**, find the file that was downloaded to your computer, and click **SEND**.
The Polycom Licensing Center responds by sending back the response.bin file.
- 8 Save the response.bin file to your local computer.
- 9 In the RealPresence Web Suite Services Portal, click **Upload File** for the portal you are activating, and upload the response file you received from the Polycom Licensing Center.
- 10 Click **ACTIVATE** to activate the licenses for the portal you are activating.
A message confirms that the license is activated.

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 license in online mode:

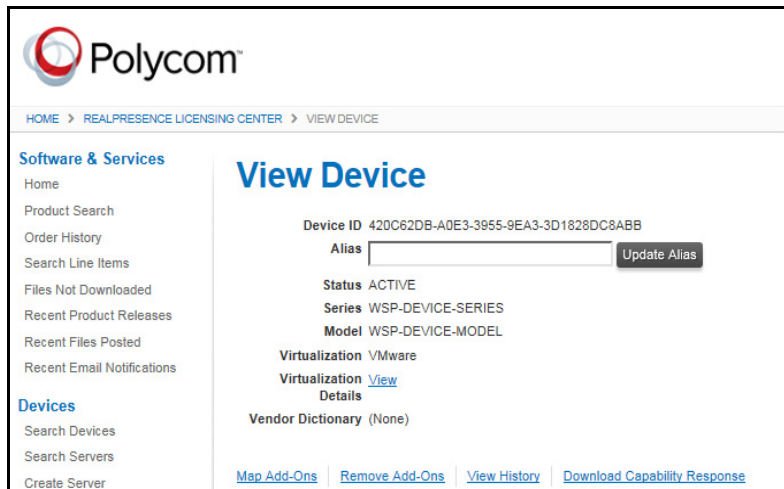
- 1 In the RealPresence Web Suite Services Portal, navigate to **Platform Settings > License**.
- 2 On the License page, click **Deactivate** next to each active license you want to deactivate. If deactivating more than one license, do so in the following order:
 - a All concurrent user licenses
 - b Enhanced Content license (if applicable)
 - c RealPresence Web Suite Experience Portal license
 - d RealPresence Web Suite Services Portal license
- 3 Call Polycom Global Services to obtain a new activation key or keys and device ID.

To deactivate a license in offline mode:

- 1 Log in to the [Polycom Licensing Center](#) with your credentials.
- 2 On the left tool bar under **Devices**, select **Search Devices**. This opens the Search Devices page.

The screenshot shows the Polycom Search Devices page. The sidebar on the left has a 'Devices' section with 'Search Devices' highlighted. The main content area is titled 'Search Devices' and contains a search form with fields for 'Device ID', 'Activation Code', and 'Alias'. A 'Filter' button is below the fields. At the bottom, there are navigation controls showing '1 to 1 of 1' and 'Entries per page: 25'.

- 3 Enter the device ID in the **Device ID** field and click **Filter**. The device ID is listed in the Device ID column.
- 4 Click the device ID that you are deactivating to open the View Device page.



Polycom™

HOME > REALPRESENCE LICENSING CENTER > VIEW DEVICE

Software & Services

Home

Product Search

Order History

Search Line Items

Files Not Downloaded

Recent Product Releases

Recent Files Posted

Recent Email Notifications

Devices

Search Devices

Search Servers

Create Server

View Device

Device ID 420C62DB-A0E3-3955-9EA3-3D1828DC8ABB

Alias **Update Alias**

Status ACTIVE

Series WSP-DEVICE-SERIES

Model WSP-DEVICE-MODEL

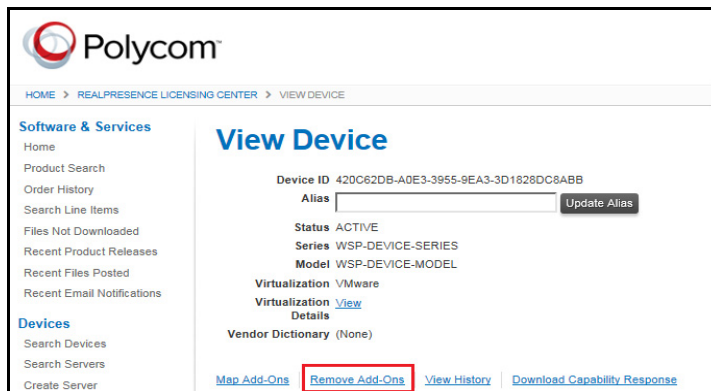
Virtualization VMware

Virtualization [View Details](#)

Vendor Dictionary (None)

[Map Add-Ons](#) [Remove Add-Ons](#) [View History](#) [Download Capability Response](#)

5 Click **Remove Add-Ons** to open the Remove Add-Ons page.



Polycom™

HOME > REALPRESENCE LICENSING CENTER > VIEW DEVICE

Software & Services

Home

Product Search

Order History

Search Line Items

Files Not Downloaded

Recent Product Releases

Recent Files Posted

Recent Email Notifications

Devices

Search Devices

Search Servers

Create Server

View Device

Device ID 420C62DB-A0E3-3955-9EA3-3D1828DC8ABB

Alias **Update Alias**

Status ACTIVE

Series WSP-DEVICE-SERIES

Model WSP-DEVICE-MODEL

Virtualization VMware

Virtualization [View Details](#)

Vendor Dictionary (None)

[Map Add-Ons](#) [Remove Add-Ons](#) [View History](#) [Download Capability Response](#)

6 In the **Quantity to Remove** field of the licenses to deactivate, enter **1**; then click **Remove Add-Ons**.



Remove Add-Ons

Device ID [420C62DB-A0E3-3955-9EA3-3D1828DC8ABB](#)

ID Type STRING

Alias

Add-Ons in Device

Add-On Description	Activation Code	Entitlement	License Term Expiration	Currently on Device	Quantity to Remove
CLOUDAXIS ST, SVCS PORTAL LICENSE	04AE-0586-F2D5-21CF	(123395227)	Permanent	1	1

Remove Add-Ons

7 On the View Device page, click **Download Capability Response**.
The response.bin file is downloaded on to the computer.

View Device

The add-ons were successfully removed.

Device ID 420C62DB-A0E3-3955-9EA3-3D1828DC8ABB

Alias Update Alias

Status ACTIVE

Series WSP-DEVICE-SERIES

Model WSP-DEVICE-MODEL

Virtualization VMware

Virtualization [View Details](#)

Vendor Dictionary (None)

[Map Add-Ons](#) |
 [Remove Add-Ons](#) |
 [View History](#) |
 [Download Capability Response](#)

- 8 On the RealPresence Web Suite Services Portal license page, click **Deactivation**.
- 9 In Upload Deactivation Response File, browse to the response file that you acquired in step 7.
- 10 Click **Yes**.

Manage Certificates and Certificate Signing Requests

The RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal servers require a secure, encrypted connection (https://) from any connected client (browser). To establish a secure connection with a browser, the RealPresence Web Suite Services Portal or RealPresence Web Suite Experience Portal must present an X.509 certificate (also known as an Secure Sockets Layer (SSL) certificate).

A self-signed certificate is sufficient to establish a secure, encrypted connection, but it does not establish trust. That is, the client does not know that the server identity is what it claims to be. Most browsers allow connection anyway, but only after presenting a warning and getting confirmation from the user to proceed. But without trust, some communications among hosts (such as between the portals, the RealPresence Access Director system, and the RealPresence DMA system) may fail.

To establish trust, the server must present a certificate digitally signed by a third-party Certificate Authority (CA) confirming the server identity. The CA is the one established by your organization IT department (issuing domain certificates) or a trusted commercial CA. But the clients connecting to the server must trust the digital signature. The trusted root certificates of the major commercial CAs are embedded in browsers, so they trust certificates signed by those CAs without any configuration needed.

Polycom recommends using trusted CA-signed certificates for the RealPresence Web Suite portals and for all other components of the RealPresence® Platform solution, including the RealPresence Access Director system. The RealPresence Access Director certificate must be signed by a trusted commercial CA, and its Subject Alternative Name (SAN) field must include the Fully Qualified Domain Name (FQDN) of the RealPresence Web Suite Experience Portal.

This section describes how to do the following:

- [Generate Certificates and Certificate Signing Requests](#)
- [View Certificates](#)
- [Copy a CSR](#)
- [Delete Certificates](#)
- [Upload Certificates or a Certificate Chain](#)
- [Configure Certificates for Reverse Proxy](#)

Generate Certificates and Certificate Signing Requests

In both the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal, you can create a Certificate Signing Request (CSR) to send to a third-party CA for a digital signature. The portals automatically put their FQDN into the CSR Common Name (CN) field. The CSRs also include the SAN field, which allows you to specify additional names (such as the portal IP address) for which the resulting certificate is valid.

**Note: The private key is not exportable**

The private key associated with a CSR is stored only on the portal that generated the CSR and cannot be exported. Therefore, the CA-signed certificate obtained from a RealPresence Web Suite Services Portal CSR cannot be used for the RealPresence Web Suite Experience Portal even if the RealPresence Web Suite Experience Portal FQDN is included in the SAN field. To use a single certificate for both portals, create the CSR in a third-party tool that makes the private key available, and submit that CSR to your CA. Upload the private key and associated CA-signed certificate to both portals. You must upload the private key first.

From your CA, obtain public key certificates for your servers and the intermediate and root certificates necessary for the certificate chain to have a complete path to the CA root certificate. All certificates must be in PEM format (Base64-encoded ASCII text). DER (binary format) certificates are not supported. If your CA provides the complete certificate chain in a single file, it must be a PEM-format P7B file (PKCS #7 protocol), not a DER-format PFX file (PKCS #12 protocol).

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

After obtaining the certificates, upload them to your portals. For instructions on uploading certificates, see [Upload Certificates or a Certificate Chain](#).

**Caution: Overwrite warning**

Before completing the following procedure, be sure that a new self-signed certificate or CSR is required. Generating a new self-signed certificate or a CSR overwrites the previous one. To check, see [View Certificates](#).

To generate a self-signed certificate or CSR in the RealPresence Web Suite Services Portal or to generate a CSR in the RealPresence Web Suite Experience Portal:

- 1 Log in to the RealPresence Web Suite Services Portal or the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **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 RealPresence Web Suite Services Portal, select one of the following: • CSR Generates a CSR to send to a third-party Certificate Authority in order to get a digitally signed public key certificate. • Certificate Generates a self-signed certificate (not applicable for the RealPresence Web Suite Experience Portal).
Type	This is set to WebServer and not changeable.

Field	Values/Description
Common Name (CN)	This is the Subject Common Name (CN) field. It defaults to the FQDN of the portal. If you leave this field blank, the CSR or self-signed certificate will not contain a CN. Note: The CN field has been deprecated by the CA/Browser Forum, but is still required by some products, notably Microsoft® Lync® Server 2013. If generating a CSR to send to a public CA, this field must not contain an internal server name or reserved (non-routable) IP address.
Organization	Enter the legally-registered name of your organization.
Organizational Unit	Enter the name of your organization unit or the DBA (doing business as) name of your organization.
Country	Enter the two-letter ISO code for the country where your organization is located.
State	Enter the full name of the state, province, or other political subdivision where your organization is located.
Location	Enter the city or locality where your organization is located.
Sub Alternate Name	This is the Subject Alternative Name (SAN) field. For a CSR, enter a comma-separated list of names that the signed certificate must cover. Because the CN field is deprecated, including the portal FQDN in the SAN field is recommended, even if the CN field contains the FQDN.

4 Click **Generate**.



Note: Use the shell to regenerate the self-signed certificate for the RealPresence Web Suite Experience Portal

To regenerate the RealPresence Web Suite Experience Portal self-signed certificate, log in to its restricted shell and run the **regenerate_certificates** command. See [Restricted Shell Commands](#). Then, restart its services or reboot the server. See [Customize the User Interface](#).

- 5 If you generated a CSR, copy it and submit it to your CA. See [Copy a CSR](#).
- 6 If you generated a self-signed certificate for the RealPresence Web Suite Services Portal, restart the rpp-tomcat and nginx services. See the following procedure.



Caution: Ensure there are no current users

Restarting web services will log out all users. The system remains inaccessible until the web services have restarted. Restart only during a maintenance window when there is no activity on the system.

To restart rpp-tomcat and nginx in the RealPresence Web Suite Services Portal:

- 1 Using an SSH client, open the RealPresence Web Suite Services Portal restricted shell using its assigned FQDN.
- 2 Log in as user *polycom* with the password you created when you first logged in to the shell to configure network settings (see the *RealPresence Web Suite Getting Started Guide*).
- 3 Restart the web-related services using the following commands:

```
service rpp-tomcat restart
service nginx restart
```



Note: Alternatively, use hypervisor tools to restart the virtual machine

In a VMware vSphere® environment, you can restart the instance using your vSphere client. In a Microsoft® Hyper-V® environment, you can use Hyper-V Manager or Windows PowerShell.

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 RealPresence Web Suite Services Portal or RealPresence Web Suite Experience Portal:

- 1 Navigate to **Platform Settings > Certificate > Certificate list**.
- 2 Click **View** next to the certificate you want to view.

Copy a CSR

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



Note: File extensions on certificate signing requests

To send a certificate signing request to a trusted CA as a file, save the file with a .csr extension.

To copy a CSR:

- 1 Log in to the RealPresence Web Suite Services Portal or the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > Certificate > Certificate list** (the RealPresence Web Suite Services Portal list is shown next).

PLATFORM			
DATE TIME CERTIFICATE LOGS SNMP MIGRATE LICENSE PROXY			
Generate CSR/Certificate Certificate list Upload Certificate			
#	Certificate Name	Component	Operation
1	webserver-own	webserver-own	VIEW
2	webserver-csr	webserver-csr	VIEW
3	__cloudax_is	webserver-trust	VIEW DELETE
4	Go_Daddy_Secure_Certificate_Authority__G2	webserver-trust	VIEW DELETE
5	localhost_localdomain	webserver-trust	VIEW DELETE

- 3 Click **View** next to the CSR.

The **Certificate Description** dialog box displays the CSR, as shown next.



- 4 Copy the entire CSR from **-----BEGIN CERTIFICATE REQUEST-----** through **-----END CERTIFICATE REQUEST-----** (include the leading and trailing dashes).
- 5 Paste the text into a text editor.
- 6 Save the file with the file extension **.csr**.
- 7 Send the file to a third-party Certificate Authority for signing.



Note: Online CSR submission

If your CA provides an online form for CSR submission, you can just paste the copied CSR into the form. You may save it as a ***.csr** file for your records.

Delete Certificates

You can delete only trust certificates.



Caution: Avoid deleting valid trust certificates

Deleting a root or intermediate certificate provided by a CA breaks the chain of trust for the public key certificate provided by that CA.

Deleting the signed public key certificate of a server that this server trusts can disrupt access to critical services.

To delete a certificate:

- 1 In the **Certificate List**, click **Delete** next to the certificate you want to delete.

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

Upload Certificates or a Certificate Chain

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

To establish secure, encrypted communication with users and verify the identity of the portal, upload the following to each portal:

- The signed public key certificate for the portal provided by the CA in response to the CSR. If the CSR was created using a third-party tool, you must first upload the associated private key.
- Any root and intermediate certificates provided by the CA to establish the chain of trust.

For servers that require secure communication, such as the Enterprise Directory server, Simple Mail Transfer Protocol (SMTP) server, and RealPresence® DMA® system, upload that server public key certificate as a trust certificate.



Caution: Select the right certificate type

When uploading a certificate, be sure to select the correct certificate type from the **Type** list to avoid possible server access problems.

The following table lists the names that the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal use for the different certificate types that you can upload. You can upload a public key certificate for a portal only if it is CA-signed.

RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal Certificate Names

RealPresence Web Suite Services Portal Name	RealPresence Web Suite Experience Portal Name	Description
WebServer Trust	CA Certificate	One of the following: • The root and/or intermediate certificates provided by a CA to establish a chain of trust for the public key certificates it signs. • The signed public key certificate of a server that this portal trusts, such as your organization Enterprise Directory SMTP server.

RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal Certificate Names

RealPresence Web Suite Services Portal Name	RealPresence Web Suite Experience Portal Name	Description
WebServer Own	Server Certificate	One of the following: - The public key certificate for this portal provided by a trusted CA in response to a CSR. - A multiple-certificate file containing the public key for this portal and the CA root and/or intermediate certificates. It must be a PEM-format P7B file (PKCS #7 protocol), not a binary (PFX) file.
WebServer Private Key	Server Key	The private key associated with the public key certificate for this portal. Note: If the public key certificate was obtained using a CSR generated by this portal, the corresponding private key is already on the portal.

**Note: Browser requirements**

Internet Explorer versions prior to version 11 are no longer supported. Use Internet Explorer 11 or another browser, such as Chrome or Firefox, to upload certificates.

To upload a certificate:

- 1 Log in to the RealPresence Web Suite Services Portal or the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > Certificate > Upload Certificate**.
- 3 From the **Type** list, select the correct certificate type.
If you have a private key to upload, you must upload it first. To successfully install the public key certificate on a portal, the corresponding private key must already be present.
- 4 Click **Browse** or **Choose File** to navigate to and select the certificate or certificate chain you want to upload.
- 5 Click **Upload**.
- 6 If you uploaded a certificate file to the RealPresence Web Suite Experience Portal, restart its services or reboot the server. See [Customize the User Interface](#).
- 7 If you uploaded a certificate file to the RealPresence Web Suite Services Portal, restart the rpp-tomcat and nginx services. See the following procedure.

**Caution: Ensure there are no current users**

Restarting web services will log out all users. The system remains inaccessible until the web services have restarted. Restart only during a maintenance window when there is no activity on the system.

To restart rpp-tomcat and nginx in the RealPresence Web Suite Services Portal:

- 1 Using a Secure Shell (SSH) client, open the RealPresence Web Suite Services Portal restricted shell using its assigned FQDN.

- 2 Log in as user *polycom* with the password you created when you first logged in to the shell to configure network settings (see the *RealPresence Web Suite Getting Started Guide*; the initial default password is *polycom*).
- 3 Restart the web-related services using the following commands:

```
service rpp-tomcat restart  
service nginx restart
```



Note: Alternatively, use hypervisor tools to restart the virtual machine

In a VMware vSphere® environment, you can restart the instance using your vSphere client. In a Microsoft® Hyper-V® environment, you can use Hyper-V Manager or Windows PowerShell.

Configure Certificates for Reverse Proxy

To configure the RealPresence Web Suite solution with reverse proxy services, upload the signed public key certificates of the RealPresence Web Suite Services Portal and the RealPresence Web Suite Experience Portal as trust certificates to the reverse proxy server (typically RealPresence Access Director).

RealPresence Web Suite Services Portal Server Settings

This section describes a number of required settings and optional customizations available in the RealPresence Web Suite Services Portal. It includes the following topics:

- [Set Web Addresses for the Portals](#)
- [Select and Configure a User Authentication Mode](#)
- [Enable Email Notifications for Users](#)
- [Configure Social Network Access](#)
- [Configure RealPresence DMA and Access Points](#)
- [Configure Conference Settings](#)
- [Update the Language Pack for the RealPresence Web Suite Services Portal](#)
- [Customize Email Templates](#)
- [Customize and White Label the User Interface](#)



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

If you make changes on a page, click **Apply** to save changes before moving to another page. If you open a new page without saving changes, the previously saved settings are applied.

Set Web Addresses for the Portals

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

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

To configure web addresses for the portals:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Core Settings > Server Settings**.
- 2 Enter addresses for the two portals as described in the following table.

Setting	Description
MEA Server	The URL using the Fully Qualified Domain Name (FQDN) assigned to the IP address of the RealPresence Web Suite Experience Portal. See the <i>RealPresence Web Suite Getting Started Guide</i> (available at Polycom Support).
WSP Server	The URL using the FQDN assigned to the IP address of the RealPresence Web Suite Services Portal. See the <i>RealPresence Web Suite Getting Started Guide</i> (available at Polycom Support).

3 Click **Update**.

After you confirm that the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal are both available and accessible using a web browser, you can continue configuring the RealPresence Web Suite Services Portal.



Note: Always use the FQDN to access the portals

Using a portal IP address to access it can cause problems. All access, whether to the user interface, administration interface, or restricted shell, must be using the FQDN, not IP address.

Select and Configure a User Authentication Mode

The RealPresence Web Suite Services Portal handles authentication for both RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal users. It can authenticate users with either Lightweight Directory Access Protocol (LDAP) or Single Sign-On (SSO). The SSO mode also allows the use of LDAP as a back-up authentication.

Set Up LDAP Authentication

You can configure a connection to the LDAP server in your organization (Microsoft® Active Directory® is supported) so that RealPresence Web Suite users can be authenticated with their LDAP-enabled accounts. With LDAP authentication enabled, all users in your Enterprise Directory are granted access to the RealPresence Web Suite Services Portal and can create, manage, and attend meetings.



Note: If the RealPresence Web Suite Services Portal domain DNS server does not point to the Enterprise Directory DNS server

If the RealPresence Web Suite Services Portal DNS server does not point to the Enterprise Directory DNS server, you need to add the SRV records of the Enterprise Directory domain controller service in the RealPresence Web Suite Services Portal domain DNS server before updating the LDAP settings configuration.

Create the SRV record in the RealPresence Web Suite Services Portal domain 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 Enterprise Directory domain controller hosting the service for domain example.com is ad_dc1.example.com, then its SRV record would be as follows:

```
_ldap._tcp.dc._msdcs.example.com. 86400 IN SRV 0 100 389 ad_dc1.example.com
```

To configure the connection to your LDAP server:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Core Settings > Authentication**.
- 2 Set **Authentication Mode** to **LDAP**.
- 3 Navigate to **Settings > Core Settings > LDAP**.
- 4 Enter information as described in the following table:

Setting	Description
Forest Root Domain	Enter the forest root domain name for the enterprise, for example polycom.com or microsoft.com.
Secure	Select to establish a secure connection to the Enterprise Directory server. This is optional, but recommended. Upload required webserver-trust certificates and restart the Apache Tomcat server to establish a secure connection with the Enterprise Directory server.
Port	Enter the port number through which LDAP communicates. The following are the port numbers for secure and non-secure connections: • Secure Port: 636 • Non-secure Port: 389
Username	Enter the user ID for the LDAP services account that has system access to the Enterprise Directory.
Password	Enter the 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 Enterprise Directory.
Use default domain for authentication	Select to use the default domain specified below as an authentication prefix.
Default Domain	Enter the name of the default domain where users are authenticated when a user ID is provided without a domain name.

- 5 Click **Update**.

Set Up Single Sign-On Authentication

With SSO enabled, users do not need to re-enter Enterprise Directory credentials on RealPresence Web Suite portals if they are already logged in to the associated Enterprise Directory domain. RealPresence Web Suite can authenticate Windows and Mac OS X users internally using the credentials they entered when they logged in to the domain.

**Note: Android and iOS devices are not supported for SSO**

The version of SSO used in this release (Simple and Protected GSSAPI Negotiation Mechanism, or SPNEGO) works only with Windows and Mac OS X devices logged in to the Enterprise Directory domain. Android and iOS devices revert to LDAP when logging in to the RealPresence Web Suite portals, and users must enter credentials.

Before you configure SSO, you must first set up a user in your Enterprise Directory domain for the RealPresence Web Suite Services Portal. The required tasks are outlined in [Appendix 2: Set Up Enterprise 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 Enterprise Directory domain.

Configure the RealPresence Web Suite Services Portal for Single Sign-On

After you set up a user in your Enterprise Directory domain for the RealPresence Web Suite Services Portal, you can configure the RealPresence Web Suite Services Portal for SSO authentication as outlined below.



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

Client devices accessing the RealPresence Web Suite Services Portal and the Enterprise Directory server must be members of the same enterprise domain in order to use SSO.

To configure the RealPresence Web Suite Services Portal for Single Sign-On:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Core Settings > Authentication**.
- 2 Set **Authentication Mode** to **SSO (Single Sign On)**.
- 3 Select the **Fallback to LDAP Authentication** check box so that users are prompted to enter their Enterprise Directory credentials if SSO is not available.

The RealPresence Web Suite Services Portal connection to the Enterprise Directory server must be configured, as described in [Set Up LDAP Authentication](#).
- 4 In the **Service Principal Name** field, enter the Service Principal Name that was created in Enterprise Directory for the RealPresence Web Suite Services Portal domain user (see [Appendix 2: Set Up Enterprise Directory for Single Sign-On](#)).
- 5 In the **Kerberos Keytab File** field, click **Upload File** to select the keytab file that was created in your Windows Enterprise Directory domain for the RealPresence Web Suite Services Portal user.
- 6 After the keytab file is successfully uploaded, click **Update**.
- 7 Restart the Apache Tomcat server as follows:
 - a Using an SSH client, open the RealPresence Web Suite Services Portal restricted shell using its assigned FQDN.
 - b Log in as user *polycom* with the password you created when you first logged in to the shell to configure network settings (see the *RealPresence Web Suite Getting Started Guide*).
 - c Enter the following command:
`service rpp-tomcat restart`

Configure User Internet Browsers to Use SSO

For users to be properly authenticated using Kerberos authentication for SSO, the following requirements must be met:

- Users must be logged in to the target Windows domain or a domain with a trust relationship with the targeted domain.
- Integrated Windows Authentication must be enabled (usually enabled by default).
- Automatic logon must be enabled in the local Intranet zone.

- The RealPresence Web Suite Services Portal must be included in the list of sites in the local intranet zone.
- For the Firefox browser, the RealPresence Web Suite Services Portal must be included in its list of trusted sites.
- For browsers configured to use a proxy server, the RealPresence Web Suite portals must be added to the exceptions list. Integrated Windows Authentication does not work through proxies.
- The time must be synchronized between the client, the RealPresence Web Suite portals, and the domain controller.

Domain administrators can push the required settings to all client computers belonging to the Enterprise Directory domain.

Enable Email Notifications for Users

Using your organizational Simple Mail Transport Protocol (SMTP) server, the RealPresence Web Suite Services Portal sends email notifications to users in the following situations:

- When the accounts are created
- When the account details are updated
- When the participants are invited to a meeting
- When the users scheduled a meeting or have been invited to is updated or canceled

This section describes how to configure the connection to the SMTP server so that it forwards these RealPresence Web Suite Services Portal emails.



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

Mail servers may have specific requirements that you need to be aware of. For example:

- Lotus Notes requires the following flag to be set to allow hosts to receive icalendar invitations: `CSAllowExternalIcalInviteToChair=1`
For details, refer to the following IBM TechNOTE:
<http://www-01.ibm.com/support/docview.wss?uid=swg21260593>
- To use Gmail™ as the SMTP server, you must turn on its option to allow access for less secure apps, located at
<https://www.google.com/settings/security/lesssecureapps>.

Refer to your mail server documentation to review its requirements for email forwarding.

To enable email notifications from the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Core Settings > SMTP**.
- 2 Enter values in the text boxes as described in the following table:

Setting	Description
Server	SMTP server FQDN or IP address.
Secure	Select to establish a secure SMTP-S/SSL connection. This is optional, but recommended if the SMTP server supports secure connection.

Setting	Description
Port	Enter the SMTP port number. Port 25 is commonly used for insecure SMTP and 587 or 465 for SMTP-S.
Login ID	The service account user ID for the SMTP service. This ID is not required for an insecure connection.
Password	The password for the service account user ID. This password is not required for an insecure connection.
Sender Mail ID	The RealPresence Web Suite system email address, which is included in the From header of all email notifications other than meeting invitations and updates. This must be a no-reply address, such as NoReply@example.com. If the SMTP server requires authentication for sending emails, this email address must be white-listed on the SMTP server.
Use sender mail ID for participant invites	Select to put the RealPresence Web Suite system no-reply email address in the From header of email meeting invitations and updates sent to invited participants. This may be necessary if the SMTP server is configured to reject messages from senders who are not authenticated users. If this option is not selected (the default), the From header of meeting invitations and updates include the email address of the host (meeting creator).
Default Reply To	By default, the Reply-To header of meeting invitations and updates include the email address of the meeting host, so that when invitees accept or reply, the response is delivered to the host. This field lets you specify a fixed address to always put in the Reply-To header. But note that doing so means meeting hosts will not receive invitee responses.

3 Click **Update**.

Configure Social Network Access

You can set up the RealPresence Web Suite environment so that users can invite contacts from their personal Google+™ accounts to meetings. With social network access enabled, users can send conference invitations to their Google+ contacts directly from the RealPresence Web Suite Services Portal.



Note: Facebook® and LinkedIn® application creation is no longer supported

Access to Facebook and LinkedIn contacts is no longer supported. To add Facebook or LinkedIn contacts to a RealPresence Web Suite meeting, users can send them an invitation by email or send the meeting details in a message on Facebook or LinkedIn.

Before enabling social network access in the RealPresence Web Suite Services Portal, you must create a custom app in Google that connects user social network contacts with the RealPresence Web Suite user environment. See [Appendix 3: Create an App to Access Google+ Social Media Contacts](#) for instructions. This application shares only contact names and presence information in the contact list. Other personal information remains private.

Enable Access to Google+ Contacts

After you create the Google app, configure access to it in the RealPresence Web Suite Services Portal.

To enable access to Google+ contacts for RealPresence Web Suite users:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Social Policy**.
- 2 Select the check box for **Google+** and complete the configuration settings as described in the following table.

Setting	Description
App ID	The unique client ID that was generated when you created the Google app.
App Secret	The client secret string that was provided to you when you created the Google app.
Auth Scope	Identifies the Google+ services to which the registered application has access: https://www.googleapis.com/auth/googletalk https://www.googleapis.com/auth/userinfo.profile https://www.googleapis.com/auth/userinfo.email https://www.googleapis.com/auth/calendar Do not edit this field unless required or advised to.
Refresh Interval	The interval at which contact and presence information is synced from Google+.

- 3 Click **Update**.

Disable Access to Social Networking Contacts

You can disable social networking contacts at any time.

To disable access to Google+ contacts in the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Social Policy**.
- 2 Clear the **Google+** check box and click **Update**.

Configure RealPresence DMA and 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 is the RealPresence Web Suite Experience Portal, a separate soft client such as RealPresence Mobile, a hardware appliance such as RealPresence Group Series, a browser, or a telephone.

RealPresence DMA systems enable the RealPresence Web Suite Services Portal to launch online video conference meetings. RealPresence Access Director systems are external links to the RealPresence DMA system that enable firewall traversal. This section explains how to configure RealPresence Web Suite to work with the RealPresence DMA and RealPresence Access Director systems.

The RealPresence Web Suite deployment requires split Domain Name System (DNS) (also known as split-horizon DNS) for correct RealPresence Web Suite Experience Portal name resolution from both inside and outside the enterprise network. Therefore, you generally must configure at least four SIP access points (the RealPresence Web Suite Services Portal requires at least one):

- Direct internal access to the RealPresence DMA system for authenticated users
- Direct internal access to the RealPresence DMA system for unauthenticated (guest) users
- External route to the RealPresence DMA system for authenticated users using the RealPresence Access Director system
- External route to the RealPresence DMA system for unauthenticated (guest) users using the RealPresence Access Director system

You can configure additional access points such as the following:

- External route to the RealPresence DMA system through H.323 video border proxy
- ISDN
- Audio dial-in through Public Switched Telephone Network (PSTN)
- External route from HTTPS Tunnel through the RealPresence Access Director system

After you add a RealPresence DMA system and its access points, the RealPresence Web Suite Services Portal connects to it and retrieves the lists of available Multi-point Control Unit (MCU) pool orders and conference templates from it. To finish configuring the RealPresence DMA system connection, you must select the MCU pool order and conference template to be used for RealPresence Web Suite conferences. See [Edit a RealPresence DMA System Connection](#).



Note: Configure the RealPresence DMA template appropriately for Enhanced Content

If you enable Enhanced Content Sharing, the RealPresence DMA template used must have **Send content to legacy endpoints** turned off to prevent clients from receiving a redundant content view in their video channel. Note, however, that this will prevent such legacy endpoints from receiving content.

Add a RealPresence DMA System and Access Points

You can configure RealPresence Web Suite to use one or more RealPresence DMA systems, each configured with multiple access points, for its meetings. The system prioritizes access points in the order in which they were added.



Note: Only one RealPresence Web Suite system per RealPresence DMA system

In an environment with multiple RealPresence Web Suite systems, such as a lab environment, each RealPresence Web Suite system must use a separate RealPresence DMA system.

To add a RealPresence DMA system and access points:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > DMA Config**.
- 2 Click **+ Another DMA**.
- 3 Enter the appropriate data for **DMA Configuration** as described in the following table. Refer to the information you entered in the “Setup Worksheet for RealPresence DMA Configuration on RealPresence Web Suite Services Portal” in the *RealPresence Web Suite Getting Started Guide* and see the example following the table.

Setting	Description
Name	A nickname for this RealPresence DMA system connection to identify it in the RealPresence Web Suite Services Portal configuration.
Host	The FQDN or IP address of the RealPresence DMA system.
Port	The TCP port number used to communicate with the RealPresence DMA system. Port 8443 is standard.
Virtual Meeting Room (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.
Common Session Initiation Protocol (SIP) Username Common SIP Password	If SIP device authentication is enabled on the RealPresence DMA system (the recommended configuration), specify the SIP device authentication credentials. The RealPresence Web Suite Services Portal provides these to devices that authenticate with it so that they can connect to the RealPresence DMA system as authorized. If Enhanced Content is enabled, these credentials are also needed by and provided to the Standards Connectors. These credentials must be in the RealPresence DMA system list of inbound device authentication entries. Callers who provide them are trusted by the RealPresence DMA system and processed by its regular dial plan. RealPresence Web Suite Experience Portal guest logins (not authenticated with the RealPresence Web Suite Services Portal) reach the RealPresence DMA system as untrusted calls (through a NoAUTH access point) and are processed by its guest dial plan. For more information, see Secure SIP Access for Guests in this guide and the <i>Polycom RealPresence DMA 7000 System Operations Guide</i> (available at Polycom Support).
Default Admin	The user ID of an admin user on the RealPresence DMA system. If the RealPresence DMA system is integrated with Enterprise Directory, this must be an Enterprise Directory user with access to all domains (not a local user defined on the RealPresence DMA system) to be able to search the VMRs of all users.
Admin Password	The password for the RealPresence DMA admin user.
Owner Domain	The domain of the user account assigned to create meetings in the RealPresence DMA system. For a local user (not in Enterprise Directory), enter LOCAL.
Owner Username	The user ID of the user account assigned to create meetings in the RealPresence DMA system.
Generate VMR From Range	Select the check box to enter the starting and ending numbers of the range to use for auto-generating random conference IDs (temporary RealPresence Web Suite VMRs). For better security, specify a wide range such as 100000 to 999999.

CORE SETTINGS		SOCIAL POLICY		DMA CONFIG		CONFERENCE SETTINGS		LANGUAGE		EMAIL		CUSTOM UI	
DMA CONFIGURATION													
Name	dma *			Default Admin	admin *								
Host	10.223.36.141 *			Admin Password	***** *								
Port	8443 *			Owner Domain	local *								
VMR Prefix	11			Owner User name	wsp *								
MCU Pool Order	WebRtc Pool Order ▼			Conference Template	WebRtc Both ▼								
Common SIP Username	wsp			☒ Generate VMR From Range 3000 to 3300 Eg. 1000 - 20001									
Common SIP Password	*****												

- 4** Click **+ Add Access Point** and enter the appropriate data as described in the following table. Refer to the setup worksheet copies that you printed out from the *RealPresence Web Suite Getting Started Guide* and completed when preparing for installation. Add access points in the order that you want the RealPresence Web Suite Services Portal to use them. For example, enter internal access points first.

Setting	Description
Location	A name for this access point that describes its location or other properties that distinguish it from other access points (such as transport and authentication).
Transport	The transport protocol associated with the access point (SIP, TUNNEL, H323, ISDN, or Public Switched Telephone Network (PSTN)).
Dial string	The dial string that an endpoint uses to dial this access point. The string must be appropriate for the specified transport type. For instance, for a SIP access point for callers outside the network, enter the public FQDN used to access the system using the RealPresence Access Director system.

Setting	Description
Auth Mode	Select one of the following options: • Shared Access point is shared by all users. Use this option if SIP device authentication is not enabled on the RealPresence DMA system. • Auth Access point is for those with enterprise credentials and who authenticate with the RealPresence Web Suite Services Portal. • Noauth Access point is for guest users who do not authenticate with the RealPresence Web Suite Services Portal. An AUTH access point requires a corresponding NoAUTH access point and vice versa.
Dial Prefix	(Optional) Specify a prefix to add to the dial string when dialing this access point. This is the prefix used by the access point to route the call or to distinguish between authenticated callers and unauthenticated guests. For instance, if this access point is for unauthenticated (guest) callers from outside the network, this is a prefix defined as an “unauthorized prefix” in the Signaling Settings page of the RealPresence DMA system. Callers whose dial string includes this prefix are processed by the RealPresence DMA system guest dial plan. For more information, see Secure SIP Access for Guests and the <i>Polycom RealPresence DMA 7000 System Operations Guide</i> (available at Polycom Support).

5 Click + Add Access Point to enter another access point as needed.

To provide access from both inside and outside the enterprise network for both authenticated and unauthenticated (guest) callers, four SIP access points are needed. See the example that follows. Access points for additional transport protocols are optional.

Location	Transport	DialString	Auth Mode	Dial Prefix	
externalAuth	SIP ▼	conf3.npicloud.org	AUTH ▼		DELETE
externalNoauth	SIP ▼	conf3.npicloud.org	NoAUTH ▼	22	DELETE
internalAuth	SIP ▼	10.223.37.10	AUTH ▼		DELETE
internalNoauth	SIP ▼	10.223.37.10	NoAUTH ▼	22	DELETE
+ ADD ACCESS POINT					
CONFIGURE CANCEL					

6 When all required access points have been added, click **Configure**.

7 Restart the RealPresence Web Suite Experience Portal. See [Customize the User Interface](#).

Edit a RealPresence DMA System Connection

After you set up a new RealPresence DMA connection, the RealPresence Web Suite Services Portal connects to it and retrieves the list of available MCU pool orders and conference templates from it. To finish configuring the new RealPresence DMA system, you must edit it to select the pool order and template to use. You can also edit a RealPresence DMA connection to change other settings if needed.

To edit an existing RealPresence DMA connection:

- 1 Click ➤ next to the RealPresence DMA entry you want to edit.
The **DMA Configuration** settings appear.
- 2 If necessary, finish configuring this RealPresence DMA connection by making the settings described in the following table.

Setting	Description
MCU Pool Order	An MCU pool order is an ordered list of pools of MCUs (conferencing bridges). Pools can be used to group MCUs by capabilities, location, or other criteria. For instance, MCUs that support WebRTC conferences must be in their own pool or pools. A pool order specifies which MCU pools may be used for a conference and their priority order. You can create a specific MCU pool order for VMRs created by the RealPresence Web Suite Services Portal to use, or you can specify an existing pool order. For RealPresence Web Suite Pro to support WebRTC, the first pool in the pool order you select must contain only WebRTC-capable MCUs. We recommend that the pool order contain <i>only</i> a pool or pools of WebRTC-capable MCUs. If the pool order contains a pool that includes non- WebRTC-capable MCUs, an MCU that is not WebRTC-capable could be selected for a conference. If that happens, clients will not be able to join using WebRTC. See the <i>Polycom RealPresence DMA 7000 System Operations Guide</i> (available at Polycom Support) for more information.
Conference Template	A conference template defines the capabilities and features of conferences based on that template. For instance, a template specifies whether WebRTC conferences are supported and to what extent (mesh, bridge, or both). You can create a specific conference template for VMRs created by the RealPresence Web Suite Services Portal to use, or you can specify an existing template. See the <i>Polycom RealPresence DMA 7000 System Operations Guide</i> (available at Polycom Support) for more information.

- 3 If necessary, make any other changes to this connection settings and access points that are required.
- 4 Verify that everything is correct and click **Configure**.

Configure Conference Settings

Conference settings control the meeting features and options available to users when they create and attend meetings.

To configure conference settings:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Conference Settings**.
- 2 Configure the conference settings as described in the following table.

Setting	Description
Personal VMR	Select one of the following options: • Schedule meetings ONLY on Personal VMR (experimental) Configures the RealPresence Web Suite Experience Portal to host only meetings using static permanent VMRs (conference IDs defined in the RealPresence® DMA® system), not meetings scheduled or started in the RealPresence Web Suite Services Portal using generated temporary VMRs. • Allow users to schedule meeting on Personal VMR and Ad-hoc VMR Select this option to enable the Use Personal VMR option on the Schedule a Meeting page. Users have the option of using their permanent personal VMR or a temporary VMR created by the RealPresence Web Suite Services Portal. • Do not allow users to schedule meeting on Personal VMR This is the default setting. All meetings scheduled or started in the RealPresence Web Suite Services Portal use temporary VMRs.
Passcode is mandatory	Select the check box to require a numeric attendee passcode for all meetings. Not available if Schedule meetings ONLY on Personal VMR is selected.
Chairperson Passcode Mandatory	Select the check box to require a numeric chairperson passcode for all meetings. Not available if Schedule meetings ONLY on Personal VMR is selected.
Expose Passcode	Select the check box to show meeting passcodes in email invitations and in the meeting URIs generated by the RealPresence Web Suite Services Portal. Not available if Schedule meetings ONLY on Personal VMR is selected. If this option is not enabled, meeting hosts must notify invitees of the meeting passcode through some other means.
Allow use of Join Meeting	Select the check box to enable the Join Meeting button on the RealPresence Web Suite Services Portal home page. This allows the user to join a meeting directly from the RealPresence Web Suite Services Portal by entering its VMR number.
Enable Calendar Invite	Select the check box to send calendar invitations when a meeting is scheduled, created, or updated. If this option is not enabled, an email is sent with a calendar invitation (*.ics) as an attachment.
AdHoc meeting duration	Enter the duration, in minutes, for Meet Now meetings. Minimum: 15 minutes; maximum: 1440 minutes (24 hours).
Buffer time before meeting starts	Specify how many minutes before its scheduled start time a meeting becomes active. Minimum: 1 minute; maximum: 60 minutes.
Buffer time after meeting ends	Specify how many minutes after its scheduled end time a meeting remains active. Minimum: 0; maximum: 120 minutes.

Setting	Description
Enhanced Content enabled	Display only. Enable or disable Enhanced Content in the RealPresence Web Suite Experience Portal administration interface. See Configure the Enhanced Content Feature .
Limit number of participants per time slot	Select the check box to limit the total number of meeting participants (including chairpersons) that can be invited to all meetings during any given time period. This lets you control to some extent how much of your video capacity (MCU resources) can be claimed by scheduled meetings. Note, however: - This feature restricts only the number of participants invited to meetings during a given time period. No control is exercised over the number of participants <i>joining</i> those meetings. - This feature restricts only RealPresence Web Suite client applications (endpoints). No control is exercised over other endpoints joining those meetings. Max participants per time slot: Specify the total number of meeting participants (including chairpersons) invited to all meetings scheduled or started for any given time period. When a user attempts to schedule a meeting or start a Meet Now meeting that would cause this limit to be exceeded, a message prompts the user to either reduce the number of participants or select a different time period. Example: - This value is set to 10. - A user schedules a meeting from 9:00 to 10:00 and invites five participants (a total of 6, including the chairperson). No other meeting is currently scheduled during that time period. - A second user attempts to schedule or start a meeting from 9:30 to 10:30, inviting four participants (a total of five, including the chairperson). Since the total number of meeting participants during the 9:30 to 10:00 time slot would be eleven, the second user cannot schedule or start that meeting without reducing the participant list by one or changing the time of the meeting.

- 3 Click **Set** to save the settings.

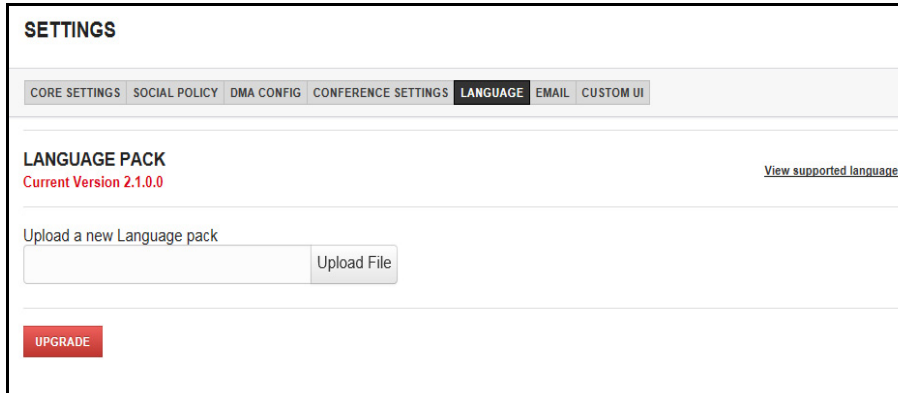
Update the Language Pack for the RealPresence Web Suite Services Portal

The RealPresence Web Suite Services Portal includes a language pack to localize the user interface. If Polycom makes a new language pack available, you can upload it to the RealPresence Web Suite Services Portal. You can upload only Polycom-authorized language packs. Contact Polycom Global Services to request a new language pack.

To upload a new language pack:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Language**.
The Language Pack page shows the current language pack version.
- 2 Click **Upload File**, browse to the new language pack file, and click **Open**.

3 Click **Upgrade**.



SETTINGS

CORE SETTINGS SOCIAL POLICY DMA CONFIG CONFERENCE SETTINGS **LANGUAGE** EMAIL CUSTOM UI

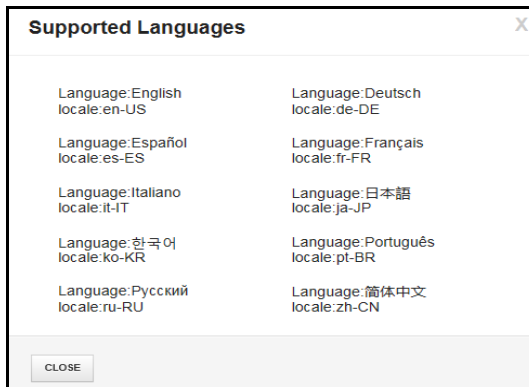
LANGUAGE PACK
Current Version 2.1.0.0 [View supported languages](#)

Upload a new Language pack

Upload File

UPGRADE

To see the languages available in the installed language pack, click **View Supported Languages**.



Supported Languages

Language: English locale: en-US	Language: Deutsch locale: de-DE
Language: Español locale: es-ES	Language: Français locale: fr-FR
Language: Italiano locale: it-IT	Language: 日本語 locale: ja-JP
Language: 한국어 locale: ko-KR	Language: Português locale: pt-BR
Language: Русский locale: ru-RU	Language: 简体中文 locale: zh-CN

CLOSE



Note: Revert to a previous language pack

After installing a new language pack, you can return to an earlier version by clicking **Revert To This Version**.

Customize Email Templates

You can customize the email 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 email templates. Only users with Super Admin privileges can edit email templates.



Caution: Edit email templates only if you understand HTML syntax

Edit email 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 the section [HTML Variables Used in Email Templates](#) to understand how the email templates are structured.

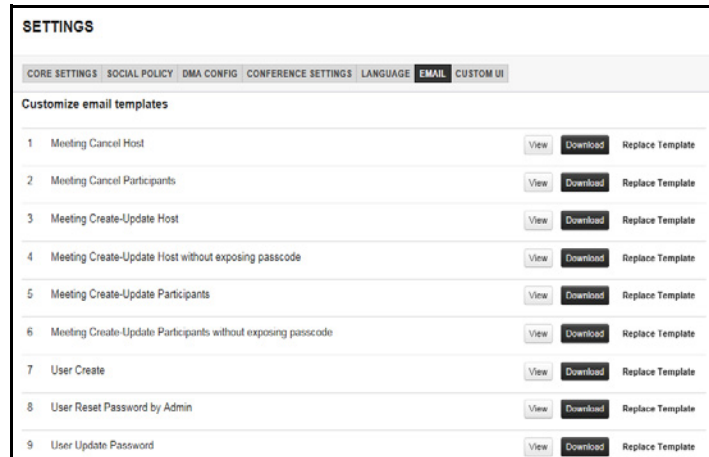
To view an email template:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Email**.

- 2 Click **View** next to the email template you want to view.
- 3 Click **Close** when done.

To download and customize an email template:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Email**.
- 2 Click **Download** next to the email template you want to download.



- 3 Click **Open with** and choose a program, or click **Save**.
- 4 Edit the template using your preferred text or HTML editor.

To replace an existing email template:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Email**.
- 2 Click **Replace Template** next to the existing template you want to replace.
- 3 Click **Select Template** and select the edited HTML file you want to upload.
- 4 Click **Preview and Upload** to view the template.
- 5 Click **Upload**.



Note: Template file size

Template files are limited to 1 MB per template. To keep the file size below 1 MB, use URL links to add images to HTML templates, and ensure that users receiving the email messages have access to the URL providing the images.

HTML Variables Used in Email 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 email templates contain references and directives that are used to specify per-instance information that can be included in an email 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 Web Suite Services Portal replaces with instance-specific details when an individual email is generated. References and directives can be added, moved, or removed, but only when they are defined as being valid for the type of email message being used.

Commonly Used Directives

The following directives are used in emails concerning user and password management.

Directives for Password Management

Directive	Description
\$FIRSTNAME	First name of the user for whom the account was created or the password was modified.
\$WSP_URL	URL of the RealPresence Web Suite Services Portal on which the account was created or the password was modified.
\$USERNAME	The user ID with which the user can log in to the RealPresence Web Suite Services Portal.
\$PASSWORD	The password with which the user can log in to the RealPresence Web Suite Services Portal.

The directives in the following table are used in emails 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 email is being sent to announce a new scheduled meeting or an update.
\$EVENT_STATUS_BODY	Set either to Created or Updated, depending on whether the email is being sent to announce a new scheduled meeting or an update.
\$CREATED_BY_NAME	The name of the user who scheduled the meeting.
\$CREATED_BY_MAIL	The email address of the user who scheduled the meeting.
\$EVENT_NAME	The name given to the meeting by the host.
\$EVENT_TIME_GMT	The scheduled start time of the meeting expressed in the UTC time standard.
\$EVENT_DURATION	The scheduled duration of the meeting.
\$EVENT_DESCRIPTION	The agenda of the meeting as entered by the host.
\$VMR	The VMR number (conference ID) for the meeting.
\$HTTPS	The secure web URL for joining the meeting.

Directives for Meeting Invitations and Cancellations (continued)

Directive	Description
\$MEETING_PASSCODE	The passcode required to join the meeting.
\$TOKEN	Encoded string that is hidden (by changing the text color to the background color) and that is read by HDX and Group Series endpoints to populate the meeting details in the calendar section of the respective device. It is located at the bottom of the page (just above the copyright) and begins as follows: 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 illustrate the use of various references and directives.

Template 7: User Create

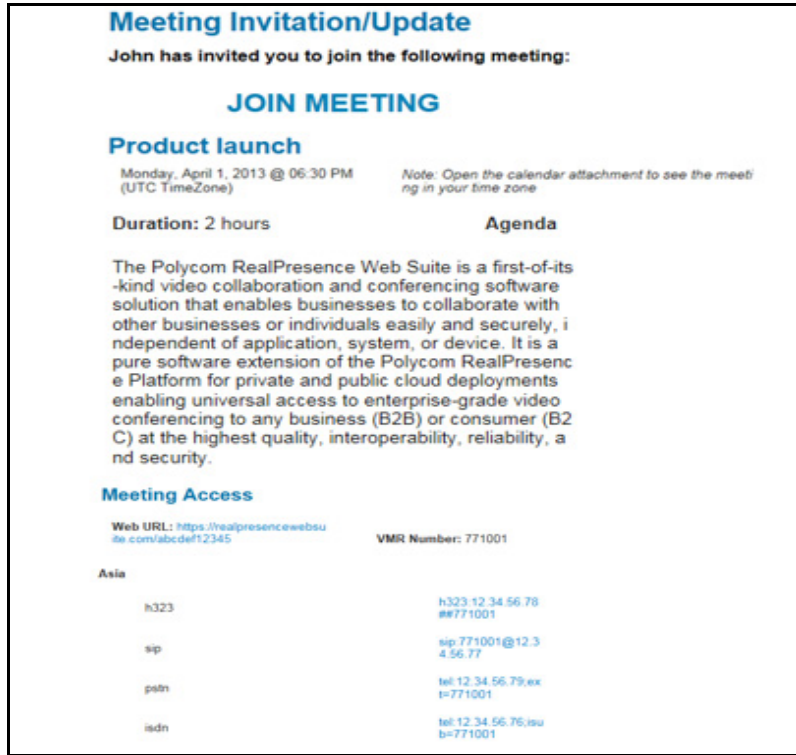
Welcome to RealPresence Web Suite

Hi John,

Your RealPresence Web Suite account has been created. Please log in with the following credentials:

Login details

Username	JohnS
Password	qwerty123
Web URL	https://realpresencewebsuite.com/

Template 6: Meeting Create-Update Participants without exposing passcode

Reset an Email Template

If you have uploaded a customized email template but want to discard it, you can reset that template to the factory default. Any template that has been edited has a **Reset** button next to it that allows you to revert to the original factory template.

Note that resetting a template deletes the customized template file that was uploaded and restores the original factory default template. To return to an earlier customized version, you must upload that version again.

To reset a template to the factory default:

- » On the **Customize email templates** page, click **Reset** next to the template you want to reset.

Customize and White Label the User Interface

You can change the background, logo, application name, favorite icon, and other information on the RealPresence Web Suite user interface to provide a custom look and display your company branding.

After you change any user interface settings in the RealPresence Web Suite Services Portal administration interface, you must apply the changes in the RealPresence Web Suite Experience Portal administration interface so that users will see the changes when they connect to the RealPresence Web Suite Experience Portal.

**Caution: Restoring settings to default**

When you edit settings, you have the option to update or restore settings to default. If you select **Restore Default**, the settings on that tab or page are restored to the settings that were in place when RealPresence Web Suite was deployed, not to the previously saved settings.

Customize the User Interface

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

- The company logo that users see at the top of the browser window.
Logos must be *.png, *.gif, or *.jpg files and no larger than 280 x 98 pixels.
- The application title that users see. The default is Polycom® RealPresence® Web Suite.
- The favorite icon displayed when the application is launched in a new tab or window.
Icons must be *.png (recommended) or *.ico files and no larger than 24 x 24 pixels.

To change the general user interface settings in the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Custom UI**.
- 2 On the **General** tab, select any of the following options:
 - **Default:** to display Polycom logo
 - **Custom:** to display your company logo
 - **Blank:** to display no logo

- 3 If you selected **Custom**, click **Select** to browse for the new logo file and click **Open**.
- 4 Set **Application Title** to **Custom**.
- 5 Type the name that your organizational users must see when they log in to schedule or attend a meeting. The maximum length for an application title is 75 characters.
- 6 Set **Fav Icon** to **Custom**.
- 7 Click **Select** to browse to the file you want to use as an icon and click **Open**.
- 8 Click **Update** to save the new UI settings.

Change the Appearance of the Login Screen

You can change the background and choose whether to display the logo or application title on the screen that users see when they log in to a RealPresence Web Suite portal.

The background file must be a *.jpg file no larger than 5 MB.

To change the login screen appearance:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Custom UI > Login Screen**.
- 2 Check or clear **Display Logo on The Login Screen** and **Display Application Title on the Login Screen** as desired.
- 3 To change the background:
 - a Set **Background** to **Custom** and click **Select**.
 - b Browse to the file you want to use and click **Open**.
- 4 Click **Preview** to verify the changes, and click **Update** to save them.

Add a Notification Message for Users

You can add a message that users see on the login screen and optionally schedule it to appear for a specific range of dates.

To display a notification message on the login screen:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Custom UI > Notification Message**.
- 2 Select **Display Message**.
- 3 Enter a title and message in the corresponding text fields.
- 4 To specify a date range during which the message is displayed, click **Schedule this Message**.
- 5 Click  to set the start and end of the date range.
- 6 Click **Update**.

Add a Logout URL

You can add a URL to which users are redirected when they log out of the system.

To add a logout URL:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Custom UI > Footer / URLs**.
- 2 Set **On Logout** to **Custom URL**.
- 3 Paste or type the address of the web page to which you want to redirect users.
- 4 Click **Update**.



Note: Logging in as an Admin or Super Admin if custom logout URL is set

If SSO is enabled and a custom logout URL is set, a user who wants to log in as an Admin or Super Admin after logging out as a standard user must use `https://<RealPresence Web Suite Services Portal address>/login/#reln`.

Change the User Interface Footer

By default, the user interface footer includes a link that displays product information and a link to the online version of the *RealPresence Web Suite User Guide*.

To change the user interface footer:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Settings > Custom UI > Footer / URLs**.
- 2 In the **On Logout** field, select **Redirect to Login Page** to navigate to the login page on logout.

- 3 To remove both the Help link and Product Info link from the user interface, clear the **Display Footer** check box.
- 4 To remove one, but not the other, clear either the **Product Info** or **Help** check box.
- 5 To direct the footer Help link to a different web page, make sure **Help** is selected, change its source setting from **Default URL** to **Custom URL**, and paste or type the address of the web page to which you want to point the Help link.
- 6 Click **Update** to apply the changes. Or
- 7 Click **Restore Default** to revert back to the default settings.

Refresh the RealPresence Web Suite Experience Portal User Interface

After you change the user interface settings in the RealPresence Web Suite Services Portal, you must refresh the user interface in the RealPresence Web Suite Experience Portal in order for it to retrieve the new settings.

To refresh the user interface in the RealPresence Web Suite Experience Portal:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Platform Settings > Custom UI** and click **Refresh**.
A message at the top of the page indicates whether the UI refresh was successful.
- 2 Log in to the RealPresence Web Suite Experience Portal as a standard user to verify that the new UI is in place.

**Note: Configure the LDAP server if not configured**

Either administrator or standard user can access the RealPresence Web Suite Experience Portal. Ensure that LDAP option is selected on the **Settings** page. If not configured, select the option **Click to configure** to configure the LDAP.

RealPresence Web Suite Services Portal Platform Settings

This section provides information on configuring certain general platform settings for the RealPresence Web Suite Services Portal. The following topics are included in this section:

- [Set the RealPresence Web Suite Services Portal Date and Time](#)
- [Generate Certificates](#)
- [Manage RealPresence Web Suite Services Portal Logging and Data Collection](#)
- [Enable SNMP Monitoring](#)
- [Migrate the Application Data](#)
- [Set Up License](#)
- [Configure HTTP Forward Proxy Settings](#)



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

If you make changes on a page, click **Apply** to save changes before moving to another page. If you open a new page without saving changes, the settings revert to the previously saved changes.

Set the RealPresence Web Suite Services Portal Date and Time

The RealPresence Web Suite Services Portal uses a Network Time Protocol (NTP) server for clock synchronization. In order for RealPresence Web Suite meetings to occur and for calls and recordings to work properly, the RealPresence Web Suite Services Portal and the RealPresence Web Suite Experience Portal must reference the same time zone and NTP servers. The default time for instances is taken from the host server. If that time is wrong, the RealPresence Web Suite Services Portal scheduler can go out of sync.



Caution: Time must be synchronized among all RealPresence Platform products

All your RealPresence Platform products, including RealPresence DMA, RealPresence Access Director, RealPresence Collaboration Server, the RealPresence Web Suite portals, and their hosts must use the same NTP servers so that time remains synchronized among them all.

If you set the time zone and NTP servers using console access after deployment, verify the time settings in the RealPresence Web Suite Services Portal administration interface. Otherwise, set them there now.

To set the date and time on the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > Date Time**.

- 2 In the **NTP Server** field, enter a space-delimited list of time servers.
- 3 In the **Time Zone** list, select the proper time zone for the system.
- 4 Click **Update**.
- 5 Restart the web-related services. See the following procedure.



Caution: Ensure there are no current users

Restarting web services will log out all users. The system remains inaccessible until the web services have restarted. Restart only during a maintenance window when there is no activity on the system.

To restart rpp-tomcat and nginx in the RealPresence Web Suite Services Portal:

- 1 Using a Secure Shell (SSH) client, open the RealPresence Web Suite Services Portal restricted shell using its assigned Fully Qualified Domain Name (FQDN).
- 2 Log in as user *polycom* with the password you created when you first logged in to the shell to configure network settings (see the *RealPresence Web Suite Getting Started Guide* (available at [Polycom Support](#)); the initial default password is *polycom*).
- 3 Restart the web-related services using the following commands:

```
service rpp-tomcat restart
service nginx restart
```



Note: Alternatively, use hypervisor tools to restart the virtual machine

In a VMware vSphere® environment, you can restart the instance using your vSphere client. In a Microsoft® Hyper-V® environment, you can use Hyper-V Manager or Windows PowerShell.

Generate Certificates

For more information on generating certificates, Certificate Signing Requests, and uploading certificates, see [Manage Certificates and Certificate Signing Requests](#).

Manage RealPresence Web Suite Services Portal Logging and Data Collection

The RealPresence Web Suite Services 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 depends on the log level selected. The more detail in a log, the more disk space required to store it, and the more system resources required to create it.

You can download all the log files on the portal as a compressed archive and view them or provide them to a Polycom Global Services representative to help resolve an issue.

With your permission, the RealPresence Web Suite Services Portal also collects usage data and sends it to Polycom to help improve the product and better serve customer needs. When you download logs, the analytics logs that include the usage data sent to Polycom are included in the log archive, so you can see what was sent to Polycom.

Set the Log Level

Logs are produced at the level of detail that you specify in Log Settings. The level of detail is greatest in All mode and least in Error mode. The system default is Info. When a log level is selected, all levels of less detailed logging are included in the information. For example, if you choose Info, the logs also include WARN and Error level information.

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.

The following table lists the log levels available on the RealPresence Web Suite Services Portal.

Log levels, from most verbose to least verbose

Log Level	Description
All	Turns on all logging.
Trace	Logs more detail than a Debug log. These logs are also helpful for debugging.
Debug	Logs fine-grained information that is 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 cause the RealPresence Web Suite Services Portal to stop 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 are troubleshooting an issue, and return the setting to Info or below for day-to-day operations. More verbose logging produces highly detailed logs that require large amounts of disk space. While highly detailed logs are useful for troubleshooting a specific problem, we do not recommend the more verbose modes for day-to-day operations.

To set the log level on the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > Diagnostics > Logs**.
- 2 Set **Level** to the logging level you want.
- 3 Click **Update** to begin logging at the selected level.

Download Log Files

To help you troubleshoot problems, you can download all the log files on the portal as a compressed archive. You can do so either from the administration interface, as described below, or from the restricted shell (see [Restricted Shell Commands](#)). A Polycom Global Services representative may request log files to assist in resolving an issue.

To download log files:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > Diagnostics > Logs**.
- 2 If necessary for troubleshooting or requested to do so by a Polycom Global Services representative, set **Level** to Debug, Trace, or All to include more detail in your logs.
- 3 Click **Update** to begin logging at the selected level. Then let the system run long enough to generate enough log information to help solve any issues that may be occurring.
- 4 Click **Download**.

The logs are saved to your Downloads folder or the location you select (depending on your browser settings) as a compressed archive file.

Enable Usage Data Collection

You can help Polycom improve RealPresence Web Suite and provide you with better support by letting the RealPresence Web Suite Services Portal send usage data to Polycom.

To continually improve the product, Polycom needs to understand how RealPresence Web Suite is used by customers. By collecting usage data, Polycom can learn more about how the system is used and which features are most important. This information guides future development and testing. If you choose not to send this information, Polycom is less aware of which features are important to you and are used by you, which may influence future development to go in directions that are less beneficial to you.

The following types of data are collected:

- License information
- Hardware configuration
- System resource usage: CPU, RAM, disk, database
- Feature usage: Social integration, enterprise directory integration, number of conferences, number of participants, count of documents uploaded
- Number of users, local and enterprise
- Security settings

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

Your decision to enable or not enable the sending of usage data does not affect the availability of any documented system feature in any way. Enabling this feature does not affect the capacity or responsiveness of the RealPresence Web Suite system.

The RealPresence Web Suite Services Portal sends usage data once per hour over a secure Transport Layer Security (TLS) connection to a Polycom collection point (`customerusagedatacollection.polycom.com`). No one outside of Polycom has access to the data received at the collection point. To avoid any impact to starting and ending calls and conferences, data is never sent between five minutes before the hour and five minutes after the hour.

To enable data collection:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > Diagnostics > Data Collection**.
- 2 Set **Automatically Send Usage Data** to **Enabled** and click **Update**.
A dialog box displays information about data collection and presents **Update** and **Cancel** buttons.
- 3 To confirm the sending of usage data to Polycom, click **Update**.

If data collection is enabled, a file named `analytics.json` contains the most recent hourly data. This file is sent to Polycom and is also included in the log archive that you can download (see [Download Log Files](#)). You can open this file in a text editor to see what was sent to Polycom.

Enable SNMP Monitoring

For more information on enabling Simple Network Management Protocol (SNMP) monitoring, see [Monitor the Environment with SNMP](#).

Migrate the Application Data

Select the option **Migrate** under **Platform Settings** to migrate all the application data from the remote system to the current system.

For more information on migrating current settings to the new RealPresence Web Suite Services Portal, see [Migrate Current Settings to the New RealPresence Web Suite Services Portal](#).

Set Up License

For more information on setting up and activating licenses, see [Activate Licenses](#).

Configure HTTP Forward Proxy Settings

In some network environment, direct access to the public Internet is blocked, and devices inside the organizational firewall must access external websites and services through a proxy server. If the RealPresence Web Suite system is deployed in such an environment, the RealPresence Web Suite Services Portal must be configured with the necessary information about the local proxy server to fulfill the following functions that require it to access the public Internet:

- Online license activation for a stand-alone RealPresence Web Suite system requires contacting the Polycom Licensing Center. For more information, see [Activate Licenses for a Stand-Alone System](#).
- Enabling end-user access to Google+™ contacts requires that the RealPresence Web Suite Services Portal communicate with the online service hosted by Google. It also requires that a client PC being used to access contacts communicate directly with the appropriate online service.

To configure forward proxy settings on the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > Proxy**.

- 2 In the **Server** and **Port** fields, enter the IP address (or FQDN) and port number for the local proxy server.
- 3 If the proxy server requires authentication, set **Authentication Proxy** to **Yes** and enter the credentials required by the proxy server into the **User ID** and **Password** fields.
- 4 Click **Update**.

To disable the use of a proxy:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > Proxy**.
- 2 Delete the entries in the **Server** and **Port** fields.
- 3 Set **Authentication Proxy** to **No**.
- 4 Click **Update**.

**NOTE: Proxy settings for user PCs**

The RealPresence Web Suite client-side social connector automatically uses the system-wide proxy settings configured in the user web browser. If the proxy requires credentials, users are prompted to enter the credentials when they access their social contacts.

Monitor the Environment with SNMP

RealPresence Web Suite can use the Simple Network Management Protocol (SNMP) to communicate data about both the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal servers to the RealPresence Platform Director system or another SNMP manager. This section describes RealPresence Web Suite SNMP support and how to configure the RealPresence Web Suite Services Portal to enable monitoring by an SNMP manager such as RealPresence Platform Director. It includes the following topics:

- [SNMP Framework](#)
- [Supported SNMP Versions](#)
- [SNMP Notifications](#)
- [Enable and Configure System Monitoring](#)

SNMP Framework

The SNMP framework includes the following parts:

- **An SNMP manager** is used to control and monitor the activities of network elements using SNMP. It makes queries to and receives notifications from SNMP agents on the managed network elements. If you have the RealPresence Platform Director system, it acts as an SNMP manager for the RealPresence Platform instances that it is configured to monitor.

The SNMP agent on the RealPresence Web Suite Services Portal and the SNMP manager to monitor it must have matching SNMP configurations in order for them to communicate.

- **An SNMP agent** resides on the network element to be monitored. It accesses the Management Information Base (MIB) data for the element and makes the data available to the SNMP manager with which it is configured to communicate.

To monitor the RealPresence Web Suite portals, you configure an SNMP agent on the RealPresence Web Suite Services Portal to communicate with an SNMP manager, such as the RealPresence Platform Director system. The SNMP agent can be configured to send notifications (traps or informs) to the SNMP manager for certain events.

- **A Management Information Base (MIB)** is a database of management information shared between the SNMP agent and manager. The MIB describes the device parameters that can be reported and managed, and stores the data for those parameters. An SNMP manager references the MIB to request data. An SNMP agent gathers and sends the data from the MIB.

Polycom systems include Polycom-specific MIBs with every system as well as third-party MIBs. Polycom MIBs are self-documenting, including information about the purpose of specific traps and inform notifications. Third-party MIBs accessible through the Polycom system may include both hardware and software system MIBs.

Supported SNMP Versions

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 SNMP agents and the management system 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 read only 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 for the agent. 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 traps.

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. The agent discards traps as soon as they are sent. It holds an inform request in memory until it receives a response 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 sent from the RealPresence Web Suite 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.

SNMP Notifications

Notification	Severity	Explanation
dmaConnectionDown	Critical	Named DMA server is unreachable.
dmaConnectionUp	Informational	Named DMA server is no longer unreachable.
wspDown	Critical	The RealPresence Web Suite Services Portal server is down.
wspUp	Informational	The RealPresence Web Suite Services Portal server is up and running.
googleConnectionDown	Critical	The Google server is unreachable.
googleConnectionUp	Informational	The Google server is no longer unreachable.
smtpConnectionDown	Critical	The Simple Mail Transfer Protocol (SMTP) server is unreachable.
smtpConnectionUp	Informational	The SMTP server is no longer unreachable.
meaConnectionDown	Critical	The RealPresence Web Suite Experience Portal server is unreachable.
meaConnectionUp	Informational	The RealPresence Web Suite Experience Portal server is no longer unreachable.

Enable and Configure System Monitoring

The following procedure enables SNMP and configures one or more SNMP notification agents on the RealPresence Web Suite Services Portal to allow the RealPresence Platform Director system or another SNMP manager to monitor the health of the RealPresence Web Suite portals.

You can implement one of the following SNMP versions:

- SNMPv2c is appropriate for standard communication models and uses a community string (global password) for authentication.
- SNMPv3 is appropriate for high-security models and requires a security user for notifications.

You can configure multiple notification agents, each with its own SNMP version, transport, notification type, and notification destination.

To enable SNMP monitoring of the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > SNMP**.
- 2 Click **Download MIB** to download a ZIP file containing the management information base for the RealPresence Web Suite Services Portal.
- 3 Import the MIB into your SNMP manager to enhance its ability to monitor the target system.
- 4 Select the **Enable SNMP Monitoring** check box.
The **Configure SNMP** fields appear.

5 Complete the applicable SNMP configuration fields, described in the following table.

The configuration selections vary depending on which SNMP version you choose.

Field	Value/Description
SNMP version	The version of SNMP (v2c or v3).
Transport	The transport protocol to be used. This is set to User Datagram Protocol (UDP) and read-only. 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 port on which the SNMP agent communicates. This is set to 161 and read-only.
Community	For SNMPv2c only. 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. Per SNMP convention, the default community string is "public," but this must be changed to make the SNMP information more secure.
Security User	For SNMPv3 only. Specifies the security name required to access a monitored MIB object.
Authentication	For SNMPv3 only. 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) Confirm Password	For SNMPv3 only. In the fields below the Authentication selection, enter and confirm the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest.
Encryption	For SNMPv3 only. Specifies the privacy protocol for the connection between the RealPresence Web Suite Services Portal and the SNMP manager. The RealPresence Web Suite Services Portal implements communication with authentication and privacy (the authPriv security level as defined in the User-based Security Model (USM) MIB). Possible values for privacy protocol are: - Data Encryption Standard (DES)—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet. - Advanced Encryption Standard (AES)—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet.
Password (for encryption) Confirm Password	In the fields below the Encryption selection, enter and confirm the encryption password to be appended to the encryption key.

Field	Value/Description
Location	Specifies the value to be returned for a standard MIB query to identify the geographical or logical location of the server.
Contact	Specifies the value to be returned for a standard MIB query to identify the name or contact information of an administrator who is responsible for the server.

6 Click **Update** to save the SNMP configuration settings.

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

8 Complete the agent configuration fields, described in the following table.

The agent configuration selections vary depending on which SNMP version you choose.



Note: Settings must match those of the targeted manager

For each notification agent, the SNMP version, transport, and notification type must be appropriate for the SNMP manager to which this agent sends notifications.

Field	Value/Definition
SNMP version	The version of SNMP (v2c or v3).
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; an inform requests acknowledgment of receipt from the SNMP manager. This field must be set in accordance with the capabilities of the SNMP manager.
IP	The IP address or Fully Qualified Domain Name (FQDN) of the SNMP manager to which this agent sends notifications.
Security User	SNMPv3 only. Select either Create New or Use Existing . If you choose Create New , select authentication and encryption protocols, along with passwords for each, as described in the preceding SNMP configuration table. If you choose Use Existing , select a user from the list of previously defined security users.

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

10 Repeat the preceding three steps to add another notification agent.

11 On the Configure SNMP page, 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 that tab or page are restored to the settings that were in place when RealPresence Web Suite was deployed.

User Management

This section provides user management information. User accounts for the RealPresence Web Suite environment (except for RealPresence Web Suite Experience Portal administrators) are managed through the RealPresence Web Suite Services Portal, where accounts can be created locally or through the Enterprise Directory domain in which the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal are members.

To set up authentication with Enterprise Directory, or to set up Single Sign-On (SSO) for users in the RealPresence Web Suite environment, see [Select and Configure a User Authentication Mode](#).

The following topics are included in this section:

- [Account Roles](#)
- [Manage User Accounts](#)

Account Roles

RealPresence Web Suite supports three account roles with different capabilities. In the RealPresence Web Suite Services Portal, each type of user sees a different menu, reflecting the tasks each user is allowed to perform. RealPresence Web Suite Experience Portal administrators are managed separately on the RealPresence Web Suite Experience Portal and all have the Super Admin role.

The following table lists the roles, their capabilities, and the menu options they see in the RealPresence Web Suite Services Portal.

RealPresence Web Suite Account Roles

Role	Primary Capabilities	RealPresence Web Suite Services Portal Menu Options
Super Admin	Manages the RealPresence Web Suite Services Portal server settings and creates and edits other Super Admin, Admin, and User accounts. The Super Admin role cannot schedule meetings. At least one Super Admin user must exist. The default Super Admin user, admin, cannot be deleted unless other Super Admin users exist. At a minimum, you must change that user account default password. For greater security, add individual administrator accounts for each authorized person and delete the generic admin account. A separate Super Admin account manages the RealPresence Web Suite Experience Portal and is maintained on that portal See Manage RealPresence Web Suite Experience Portal Users.	User Management Settings Platform Settings
Admin	Creates and manages Admin accounts, User accounts, and online video conference meetings. The administrator cannot change server settings or create and manage Super Admin accounts. Upon login, an Admin user initially sees the same home page as regular users, but can access the administration interface by clicking Admin in the menu panel on the right.	Schedule Calendar Address Book User Management
User	Creates, manages, and attends online video conference meetings.	Schedule Calendar Address Book

Manage User Accounts

This section includes the following topics on managing user accounts:

- [Required Internal System User Accounts](#)
- [Change Your Password](#)
- [Create User Accounts](#)
- [Edit User Accounts](#)
- [Delete User Accounts](#)
- [Reset User Passwords](#)

Required Internal System User Accounts

The following table lists the internal system user accounts that cannot be deleted. These accounts are used by various system processes for inter-portal communications.


Caution: Set secure passwords for the internal system user accounts

Change the default passwords for the internal system user accounts as soon as possible. Failure to change them could allow someone to log in to the RealPresence Web Suite Services Portal with Super Admin privileges. To change the password for an internal system user account, you must first edit that account and add an email address to which the RealPresence Web Suite Services Portal can send notifications of account changes.

Required RealPresence Web Suite Internal System User Accounts

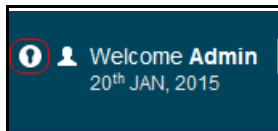
Internal System User	Description
meaconf	Used for conference communication with the RealPresence Web Suite Experience Portal. (Default password = <i>meaconf</i>)
meaauth	Used for authentication communication with the RealPresence Web Suite Experience Portal. (Default password = <i>meaauth</i>)
measys	Used for license communication with the RealPresence Web Suite Experience Portal. (Default password = <i>measys</i>)
ecsparticipant	Used for enhanced content sharing communication between the RealPresence Web Suite Experience Portal and the Standards Connectors. Only used if the Pro license is present and the Enhanced Content feature is enabled. (Default password = <i>ecsparticipant</i>)

Change Your Password

When you are logged in to the RealPresence Web Suite Services Portal administration interface, you can change your password at any time.

To change your RealPresence Web Suite Services Portal administrator password:

- 1 Log in to the RealPresence Web Suite Services Portal with Super Admin credentials. Or log in with Admin credentials and click **Admin** in the menu bar on the right to access the administration interface.
- 2 Click  beside the welcome message in the upper right-hand corner of the administration interface, as shown next.



- 3 Enter your current password, the new password, and confirm the new password.
- 4 Click **Change**.

Create User Accounts

Super Admin and Admin users can create RealPresence Web Suite accounts for Enterprise Directory users or locally in the RealPresence Web Suite Services Portal. This section describes both how to add Enterprise Directory users and how to create local accounts.

Add Enterprise Directory Users

If the RealPresence Web Suite Services Portal is connected to the organizational Enterprise Directory (Lightweight Directory Access Protocol (LDAP) authentication is enabled), all users in your Enterprise Directory are granted access to the RealPresence Web Suite Services Portal and can create, manage, and attend online video conference meetings. Confirmation emails are not sent when Enterprise Directory users are imported. These imported users are enabled automatically with the User role and remain enabled until their accounts are disabled. They do not automatically appear in the RealPresence Web Suite Services Portal user list.

You only need to add an Enterprise Directory user to the list manually in order to change the user role or disable the user access to RealPresence Web Suite.

To manually add an Enterprise Directory user to the RealPresence Web Suite Services Portal list of users:

- 1 In the RealPresence Web Suite Services Portal administration interface, click **User Management**.
- 2 On the **Users** page, shown next, click **+ LDAP User**.

- 3 In the **Import Active Directory Users** search field, enter the first name, last name, or user name of the user you want to find and press **ENTER**.

You can search for a portion of a name. Use an initial wildcard character (*) if the string for which you are searching is not at the beginning of the name. For instance, rob finds Robert, Robyn, Robles, and Robinson; *bert finds Robert, Alberto, Bert, Robertson, and Colbert.

- 4 Select the user you want to add and click **Add**.

To change an Enterprise Directory account user role or disable the user in RealPresence Web Suite, see [Edit an Account Imported from Enterprise Directory](#).

Add Local Users

In the RealPresence Web Suite Services Portal, Super Admin and Admin users can add other local users. This section describes how to create local accounts.

To add local users in the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Services Portal administration interface, click **User Management**.
- 2 On the **Users** page, click **+ User**.
- 3 Type the relevant user information in the text boxes provided.
- 4 Set **User Role** to the desired user type. For more information on user types, see [Account Roles](#).
- 5 Click **Add**. An email is sent to the newly created user containing his or her user name, password, and URL.

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

Edit User Accounts

The RealPresence Web Suite Services Portal enables Admin and Super Admin users to edit accounts imported from the Enterprise Directory or created locally. You can edit all fields for a local account, but you can change only two settings—role type and enable/lock—in an account imported from Enterprise Directory.

Edit an Account Imported from Enterprise Directory

For user accounts imported from Enterprise Directory, you can only change the user role or disable the user account. Only a Super Admin can change a role type to Super Admin or edit a Super Admin account.

To edit a user account imported from the Enterprise Directory:

- 1 In the RealPresence Web Suite Services Portal administration interface, click **User Management**.
- 2 Use the search field to find the user you want to edit. Enter any portion of a name, user ID, or email address and press **ENTER** to display the matching users.
- 3 Click  to the right of the user you want to edit.
- 4 In the **Edit User** dialog, do one of the following:
 - Set **User Role** to a different role type.
 - Clear the **Enable User** check box to disable the user account, or check it to re-enable a disabled user account.
- 5 Click **Save**.

Edit a Locally Created User Account

All of the fields in a locally created account can be edited. Only a Super Admin can change a role type to Super Admin or edit a Super Admin account. For more information on user types, see [Account Roles](#).

To edit a local user account:

- 1 In the RealPresence Web Suite Services Portal administration interface, click **User Management**.
 - 2 Use the search field to find the user you want to edit. Enter any portion of a name, user ID, or email address and press **ENTER** to display the matching users.
 - 3 Click  to the right of the user you want to edit.
 - 4 In the **Edit User** dialog, do any of the following:
 - Edit any of the fields that need to be changed.
 - Set **User Role** to a different role type.
 - Clear the **Enable User** check box to disable the user account, or check it to re-enable a disabled user account.
 - 5 Click **Save**.
- An email containing the user name, 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 regular User accounts. Admins can delete only other Admin and regular User accounts. For more information on user types, see [Account Roles](#).

To delete a user account:

- 1 In the RealPresence Web Suite Services Portal administration interface, click **User Management**.
- 2 Use the search field to find the user you want to delete. Enter any portion of a name, user ID, or email address and press **ENTER** to display the matching users.
- 3 Click the **X** to the right of the user you want to delete.
- 4 When prompted to confirm, click **Delete** to remove the user.

Reset User Passwords

An Admin or a Super Admin can reset a user password. This provides greater security by preventing former or unauthenticated members of your organization from being able to log in to the RealPresence Web Suite Services Portal.



Caution: Check the user email address before resetting the password

Unless you want to lock out a user, be sure the account has a valid email address before resetting the password. If you do want to lock out a user, be sure there is no valid email address for the account.

To reset a password:

- 1 In the RealPresence Web Suite Services Portal administration interface, click **User Management**.
- 2 Use the search field to find the user you want. Enter any portion of a name, user ID, or email address and press **ENTER** to display the matching users.
- 3 Click the **i** to the right of the user whose password you want to reset.
- 4 In the **Change this user's password** dialog box, enter a new password in the **Password** field, and click **Change**. Or leave the field blank to assign the user a generated password unknown to you.
If the account has an email address, an email containing the new password is sent to the user.

RealPresence Web Suite Experience Portal Conference Settings

After you deploy the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal as described in the *RealPresence Web Suite Getting Started Guide* (available at [Polycom Support](#)), activate licenses, install certificates, and configure the RealPresence Web Suite Services Portal (see [Summary of Initial Setup Tasks](#) for an overview of the tasks), you are ready to configure the RealPresence Web Suite Experience Portal for conferencing in your Polycom RealPresence environment.

This section describes how to do the following:

- [Enable the RealPresence Web Suite Experience Portal for Conferencing](#)
- [Configure the RealPresence Web Suite Experience Portal Conference Authentication Settings](#)
- [Configure the RealPresence Web Suite Experience Portal Conference Agents and Settings](#)
- [Update the Language Pack for the RealPresence Web Suite Experience Portal](#)
- [Manage the RealPresence Web Suite Experience Portal User Roles](#)



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

If you make changes on a page, click **Apply** to save changes before moving to another 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 Web Suite Experience Portal, make sure to restart the portal services or server. See [Customize the User Interface](#) for instructions.

Enable the RealPresence Web Suite Experience Portal for Conferencing

You must enable the RealPresence Web Suite Experience Portal and set its secure and non-secure web addresses. Note that the terms “external” and “internal” for these settings do not refer to outside or inside the network. The “external” addresses enable human users to access the portal, and the “internal” addresses enable the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal to communicate with each other on the network.

The web addresses must be URLs using the Fully Qualified Domain Name (FQDN) of the RealPresence Web Suite Experience Portal.



Note: Internal addresses must resolve to the RealPresence Web Suite Experience Portal IP address

If your internal Domain Name System (DNS) resolves the RealPresence Web Suite Experience Portal FQDN to an IP address other than the RealPresence Web Suite Experience Portal (for instance, to the external IP address of your RealPresence Access Director), you must define a second FQDN in your internal DNS that resolves to the RealPresence Web Suite Experience Portal IP address and assign that FQDN to the internal addresses used for inter-agent communication.

To enable the RealPresence Web Suite Experience Portal for conferencing:

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Conference > General Settings**.
- 3 Select **RealPresence Web Suite Experience Portal enabled**.



Note: Options for Enhanced Content enabled and Endpoint control enabled

For more information regarding the options **Enhanced content enabled** and **Endpoint control enabled**, see [Configure the Enhanced Content Feature](#) and [Configure the Resource Manager Authentication Agent](#).

- 4 Enter the **Web Addresses** settings as described in the following table.

Setting	Description
Secure External Address	The HTTPS address that Enhanced content enabled selected by the users to connect to the RealPresence Web Suite Experience Portal.
External Address (non-secure)	The HTTP address that the users use to connect to the RealPresence Web Suite Experience Portal. By default, it reroutes to the secure external address.
Secure Internal Address	The address used for inter-agent communication between the servers (not for users). This address includes the port number through which the portals connect to the Apache Tomcat server. By default, this is port 8443.
Internal Address (non-secure)	The non-secure address used for the inter-agent communication between the servers (not for users). By default, it reroutes to the secure internal address.

- 5 Click **Apply**.
- 6 To implement the RealPresence Web Suite Experience Portal conference settings, navigate to **Platform Settings > Restart** and click **Reboot Server**.

Configure the RealPresence Web Suite Experience Portal Conference Authentication Settings

The authentication settings in the RealPresence Web Suite Experience Portal include the rules used to authenticate users and guests to enable them to host or attend meetings and the authentication agent configurations.

Set Authentication Rules

Authentication rules are made up of three settings: *Match*, *Property*, and *Realm*.

To set authentication rules for the RealPresence Web Suite Experience Portal:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Conference > Authentication**.
- 2 Complete the fields in the **Match**, **Property**, and **Realm** columns, as described in the following table.

Setting	Description
Match	A regular expression that reflects the way you want the property to match for authentication. This value can reflect a host, domain host, or email domain. For example, to authenticate only users with a polycom.com email address, enter the following regular expression to match against the UserAddressDomain property: <pre>:+@(polycom.+)\$</pre>
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 Match the provided regular expression against the source of authentication for single sign-on users. • SSOUsername Match the provided regular expression against the address of the RealPresence Web Suite Services Portal. • UserAddressDomain Match the provided regular expression against the email domain for users. • Host Match the provided regular expression against the host URL to set the realm.
Realm	The target authentication realm is the FQDN of the RealPresence Web Suite Services Portal server that you want to authenticate users against. UserAddressDomain and SSOSource can point to realms in the RealPresence Web Suite Services Portal authentication agent realm list using \$#, with \$1 referencing the first element in the list, and so on.

- 3 To add a rule, click .
- 4 To change the priority of a rule, click  to its left and drag it up or down.
Authentication matching starts at the first rule, moves down the list, and stops when the user authentication method matches a listed rule.
- 5 Click **Apply**.

Configure the RealPresence Web Suite Services Portal Authentication Agent

The RealPresence Web Suite Experience Portal queries the RealPresence Web Suite Services Portal to authenticate users logging in to it to join a conference. Configure settings for the authentication agent in the RealPresence Web Suite Experience Portal to enable it to communicate with the RealPresence Web Suite Services Portal.

To configure the authentication agent that communicates with the RealPresence Web Suite Services Portal:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Conference > Authentication**.
- 2 Under **Agents**, expand the **RealPresence Web Suite Services Portal Authentication** settings.
- 3 Complete the settings as described in the following table.

Setting	Description
Target URL	The FQDN of the RealPresence Web Suite Services Portal (https:// included).
Username	Read only. The name of the internal system user responsible for authentication, <i>meaauth</i> .
Password	Click [!] to enter the password for the <i>meaauth</i> user. The default is <i>meaauth</i> , which must be changed for security reasons. See Required Internal System User Accounts .
Enforce Certificate Validation	Select to require the RealPresence Web Suite Services Portal to present a valid certificate. Polycom recommends using trusted Certificate Authority (CA)-signed certificates for the RealPresence® Web Suite® portals and for all other components of the RealPresence® Platform solution.
Realms	Enter the RealPresence Web Suite Services Portal FQDN and the domains that the authentication rules can authenticate users against, separated by commas.
Allow domain users to bypass authentication and use guest login	Select the check box to enable the Join as guest option on the RealPresence Web Suite Experience Portal login page, allowing authorized users who would normally be authenticated by the RealPresence Web Suite Services Portal to join a meeting as a guest instead of as an authenticated user.
Default Login Method (experimental)	If Enterprise is selected (the default), the RealPresence Web Suite Experience Portal login page requests user enterprise login credentials. Select Guest to default the login page to Join as guest mode. The Guest setting is intended to accommodate scenarios where the RealPresence Web Suite Services Portal is not being used for authentication or where the number of guest users is so large that making it the default is desirable.

- 4 Click **Apply**.

Configure the Resource Manager Authentication Agent

Configuring the authentication agent that communicates with RealPresence Resource Manager is necessary in order to enable Polycom Concierge in your RealPresence Platform environment.

Polycom Concierge makes it possible for users of personal devices (computer or smart phone) running RealPresence Mobile or RealPresence Desktop to pair their personal device with a Polycom room endpoint and join a meeting. The paired device can perform advanced collaboration and control functions such as

meeting roster, recording, and endpoint control. A paired device running RealPresence Desktop can share and receive enhanced content (Polycom Concierge requires RealPresence Web Suite Pro with Enhanced Content enabled).

To enable the Polycom Concierge solution, RealPresence Web Suite, RealPresence DMA, RealPresence Resource Manager, Enterprise Directory, and Exchange Server must all be properly configured. For complete solution deployment information, see the *Polycom Concierge Solution Deployment Guide*.

Polycom Concierge client systems connect to the RealPresence Web Suite Experience Portal to gain access to the solution services. The RealPresence Web Suite Experience Portal must be able to communicate with the RealPresence Resource Manager system, which provisions and manages both the room endpoints and the personal device client software. Configure settings for the Resource Manager agent to enable this communication.

To configure the authentication agent that communicates with RealPresence Resource Manager:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Conference > General Settings** and select **Endpoint control enabled**.
- 2 Navigate to **Conference > Authentication**.
- 3 Under **Agents**, expand the **Resource Manager** settings.
- 4 Select **Enabled**.
- 5 Complete the settings as described in the following table.

Setting	Description
Target URL	The URL for accessing the RealPresence Resource Manager REST API. For instance, if the RealPresence Resource Manager FQDN is <code>rprm.example.com</code> , the URL for accessing the API would be: <code>https://rprm.example.com/api/rest</code>
Username	The user ID for accessing the RealPresence Resource Manager API.
Password	Click [!] to enter the password for Username .
Enforce Certificate Validation	Select the check box to require RealPresence Resource Manager to present a valid certificate. Polycom recommends using trusted CA-signed certificates for the RealPresence Web Suite portals and for all other components of the RealPresence Platform solution.
Realms	Enter the RealPresence Resource Manager FQDN and the domains that the authentication rules can authenticate users against, separated by commas.
Allow domain users to bypass authentication and use guest login	Select the check box to allow authorized users who would normally be authenticated in the RealPresence Resource Manager to join a meeting as a guest instead of as an authorized user.

- 6 Click **Apply**.

Configure the RealPresence Web Suite Experience Portal Conference Agents and Settings

In order for the RealPresence Web Suite Experience Portal to host meetings, you must configure the agent that communicates with the RealPresence DMA system and the conference agent and settings.

In a normal RealPresence Web Suite deployment, in which conferences can be scheduled or started in the RealPresence Web Suite Services Portal, you must select and configure **Allow scheduled and static meetings** under **Conference Settings**. This setting supports both temporary Virtual Meeting Rooms (VMRs) (the *lobby code* created when a meeting is scheduled or started in the RealPresence Web Suite Services Portal) and permanent VMRs (the *Conference ID* created in the RealPresence DMA system). In both cases, the RealPresence Web Suite Experience Portal conference agent queries the RealPresence Web Suite Services Portal for meeting information; the RealPresence Web Suite Services Portal queries the RealPresence DMA system when necessary.

Do not select and configure the **Allow only static meetings** conference agent unless the RealPresence Web Suite Experience Portal hosts *only* meetings using permanent VMRs (Conference IDs defined in the RealPresence DMA system), not meetings scheduled or started in the RealPresence Web Suite Services Portal. If **Allow only static meetings** is selected, the RealPresence Web Suite Experience Portal does not query the RealPresence Web Suite Services Portal for meeting information, and callers will not be able to join a meeting using a temporary VMR created by the RealPresence Web Suite Services Portal.

Review Conference Lobby Rules

Lobby rules define which of two internal routes are used for a meeting request, based on what the dial string matches. Two lobby rules are available by default, and those two are correct and sufficient for a normal RealPresence Web Suite deployment. Do not change these rules or add a rule without consulting Polycom Global Services first.

To review or change the lobby rules for the RealPresence Web Suite Experience Portal:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Conference > Conference**.
- 2 To change a rule, edit the fields in the **Match**, **Property**, and **Route** columns, described in the following table.

This must not be necessary. If you believe your unique environment requires changes to a rule, consult with Polycom Global Services.

Setting	Description
Match	A regular expression that matches the dial strings to be handled by the specified route. The default regular expression for the <code>adhoc.cloudaxis.local</code> route matches any numeric VMR. This is the rule used for a meeting initiated when a user logs into the RealPresence Web Suite Experience Portal and enters a permanent (static) VMR number (a Conference ID defined in the RealPresence DMA system). The default regular expression for the <code>scheduled.cloudaxis.local</code> route matches any alphanumeric VMR. This is the rule used for a meeting that a user either scheduled or initiated (using the Meet Now function) in the RealPresence Web Suite Services Portal.
Property	What the match expression is applied to. This must be <i>lobbycode</i> (the VMR in the dial string).
Route	The internal route used for calls that match this rule. Two routes exist: <code>adhoc.cloudaxis.local</code> for permanent (static) VMRs defined in the RealPresence DMA system <code>scheduled.cloudaxis.local</code> for temporary VMRs defined in the RealPresence Web Suite Services Portal

- 3 To add a rule, click  and complete the fields in the **Match**, **Property**, and **Route** columns.
This must not be necessary. If you believe your unique environment requires another rule, consult with Polycom Global Services.
- 4 To change the priority of a rule, click  and drag it up or down.
- 5 Click **Apply**.
- 6 To implement the lobby rule configuration changes, navigate to **Platform Settings > Restart** and click **Reboot Server**.

Configure the RealPresence DMA Agent

All conference room requests get routed through the RealPresence DMA system that RealPresence Web Suite is configured to use (see [Add a RealPresence DMA System and Access Points](#)). The RealPresence DMA system also manages the meeting roster and controls recordings. The RealPresence DMA agent on the RealPresence Web Suite Experience Portal communicates with the RealPresence DMA system to obtain meeting rosters and manage rosters and recording.

To configure the RealPresence DMA agent:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Conference > Conference**.
- 2 Under the **Agents** heading, click **DMA** and configure the agent that communicates with the RealPresence DMA system, as described in the following table.

Setting	Description
Target URL	The FQDN or IP address of the RealPresence DMA server, using this syntax: <code>https://<IP address or FQDN of RealPresence DMA>:8443/api/rest</code>
Username	The user ID of an admin user on the RealPresence DMA system. This must be the same as the admin user entered in the DMA Configuration section of the RealPresence Web Suite Services Portal. If the RealPresence DMA system is integrated with Enterprise Directory, this must be an Enterprise Directory user (see Add a RealPresence DMA System and Access Points).
Password	The password for the RealPresence DMA admin user.
Enforce Certificate Validation	Select the check box to require that the RealPresence DMA system present a valid certificate. Polycom recommends using trusted CA-signed certificates for the RealPresence Web Suite portals and for all other components of the RealPresence Platform solution.
Routes	This field includes the conference routes specified in the conference lobby rules (see Review Conference Lobby Rules), <code>scheduled.cloudaxis.local</code> and <code>adhoc.cloudaxis.local</code> . Do not make any changes.
Prefix	Enter the dialing prefix, if any, for the RealPresence DMA system.

- 3 Click **Apply**.
- 4 To implement the RealPresence DMA agent configuration changes, navigate to **Platform Settings > Restart** and click **Reboot Server**.

Configure the Conference Agent and Settings

For most RealPresence Web Suite deployments, the conference settings type must be **Allow scheduled and static meetings**. It supports both temporary VMRs (created when a meeting is scheduled or started in the RealPresence Web Suite Services Portal) and permanent VMRs (created in the RealPresence DMA system).

With **Allow scheduled and static meetings** selected, the conference agent communicates with the RealPresence Web Suite Services Portal to retrieve meeting information. If the RealPresence Web Suite

Services Portal does not have the information for the VMR requested, it queries the RealPresence DMA system.

The **Scheduled Conference Settings** determine which options are available to users attending these meetings and how calls are routed to them.



Caution: For a normal deployment, do not select static only

Under **Conference Settings**, do not select **Allow only static meetings** unless the RealPresence Web Suite Services Portal is not used to schedule or start meetings, and the RealPresence Web Suite Experience Portal hosts *only* meetings using permanent VMRs (Conference IDs defined in the RealPresence DMA system).

If **Allow only static meetings** is selected, the RealPresence Web Suite Experience Portal queries the RealPresence DMA system for meeting information instead of querying the RealPresence Web Suite Services Portal. Callers will not be able to join a meeting using a temporary VMR created in the RealPresence Web Suite Services Portal.

To configure the scheduled and static conference agent:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Conference > Conference**.
- 2 Expand **Conference Settings** and set **Type** to **Allow scheduled and static meetings**.
- 3 Expand **Scheduled Conference Settings**.
- 4 Complete the settings as described in the following table.

Setting	Description
Target URL	The complete URL of the RealPresence Web Suite Services Portal server (including https://).
Username	Read only. The name of the internal system user responsible for conferences, <i>meaconf</i> .
Password	Click [!] to enter the password for the <i>meaconf</i> user. The default is <i>meaconf</i> , which must be changed for security reasons. See Required Internal System User Accounts .
Enforce Certificate Validation	Requires the RealPresence Web Suite Services Portal to present a valid certificate. Polycom recommends using trusted CA-signed certificates for the RealPresence Web Suite portals and for all other components of the RealPresence Platform solution.
Routes	This field contains the conference routes specified in the conference lobby rules (see Review Conference Lobby Rules), <code>scheduled.cloudaxis.local</code> and <code>adhoc.cloudaxis.local</code> . Do not make any changes.

- 5 Expand **Settings** and complete the settings that govern meetings as described in the following table.

Setting	Description
Allow Anonymous Participants	If selected, users can attend meetings without being authenticated against the RealPresence Web Suite Services Portal. If not selected, unauthenticated users are blocked from attending meetings.
Show End Meeting options	Provides chairpersons with the option to leave the meeting (letting it continue) or end the meeting for all.
Require Display Name	Prompts anonymous attendees to enter a name before joining a meeting.
Media Preferences	Adjust the default call rate settings based on available bandwidth in your environment. We recommend matching the settings in the conference template. • 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. This value must be set lower than the value for non-tunneled calls.

By itself below the **Settings** section, the **Description** setting specifies the description displayed at the top of the meeting window for meetings started in the RealPresence Web Suite Experience Portal. The default is Virtual Meeting Room {{ LobbyCode|getvmr }}.

- 6 Optionally, change Virtual Meeting Room to the desired description. Do not change the conference ID placeholder, {{ LobbyCode|getvmr }}, unless you do not want the VMR number to be displayed.
- 7 Expand **External Conference Template** and specify the settings for each access point in your RealPresence Web Suite environment, as described in the following table. These settings must match the settings for each access point set up in the RealPresence Web Suite Services Portal (see [Add a RealPresence DMA System and Access Points](#)).

Two sets of access point fields containing sample values are present by default. Edit those for your first two access points.

Setting	Description
Dial String	The dial string that an endpoint uses to dial this access point. The string must be appropriate for the specified access point transport type (for example, sip: for SIP). Do not remove or change the conference ID placeholder, {{ LobbyCode getvmr }}, but precede it with the appropriate dial prefix for this access point, if any.
Location	A name for this access point that describes its location or other properties that distinguish it from other access points (such as transport and authentication). Use the same name specified in the RealPresence Web Suite Services Portal for this access point.
POP Address	The FQDN or IP address of the server/device to which callers dialing this access point are connected. This generally matches the value entered after the @ sign in the dial string above.

Setting	Description
Transport	The transport protocol for this access point (Session Initiation Protocol (SIP), TUNNEL, H323, ISDN, or Public Switched Telephone Network (PSTN)).
Authentication Mode	Select one of the following options: • SHARED Access point is shared by all users. Use this if SIP device authentication is not enabled on the RealPresence DMA system. • AUTH Access point is for those with enterprise credentials and who authenticate against the RealPresence Web Suite Services Portal. • NOAUTH Access point is for guest users who do not authenticate against the RealPresence Web Suite Services Portal.

- 8 To add another access point, click the  below **Authentication Mode** and complete the new set of access point fields as described in the preceding table. Repeat if necessary.
- 9 Leave the **Conference ID** field set to the Conference ID placeholder, `{{ LobbyCode|getvmr }}`.
- 10 If SIP device authentication is enabled on the RealPresence DMA system (the recommended configuration), for **Shared Credentials** specify the SIP device authentication credentials. The RealPresence Web Suite Experience Portal provides these to devices that it has authenticated by querying the RealPresence Web Suite Services Portal (see [Configure the RealPresence Web Suite Services Portal Authentication Agent](#)) so that they can connect to the RealPresence DMA system as authorized.

These credentials must be in the RealPresence DMA system list of inbound device authentication entries. Callers who provide them are trusted by the RealPresence DMA system and processed by its regular dial plan.

RealPresence Web Suite Experience Portal guest logins (not authenticated with the RealPresence Web Suite Services Portal) reach the RealPresence DMA system as untrusted calls (using a NoAUTH access point) and are processed by its guest dial plan.
- 11 Click **Apply**.
- 12 To implement the conference settings configuration changes, navigate to Platform Settings > **Restart** and click **Reboot Server**.

Configure the WebRTC Agent

RealPresence Web Suite Pro can be configured to support Web Real-Time Communication (WebRTC), but the WebRTC solution depends on proper configuration of multiple RealPresence Platform components. Enabling WebRTC in RealPresence Web Suite Pro is the final step in the solution deployment process.

Before enabling the RealPresence Web Suite Experience Portal for WebRTC support by configuring its WebRTC agent, you must enable and configure WebRTC across the RealPresence Platform products in order to implement support for it. Refer to [Appendix 1: Deploy the WebRTC Solution](#) for a complete description of the Polycom WebRTC solution, the required solution components, and the procedures for enabling WebRTC on each component, including the RealPresence Web Suite Experience Portal.

Update the Language Pack for the RealPresence Web Suite Experience Portal

The RealPresence Web Suite Experience Portal includes a language pack to localize the user interface. If Polycom makes a new language pack available, you can upload it to the RealPresence Web Suite Experience Portal. You can upload only Polycom-authorized language packs. Contact Polycom Global Services to request a new language pack.

The language pack versions used in the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal must match.

To upload a new language pack:

- 1 In the RealPresence Web Suite Experience Portal administration interface, click **Language**.
- 2 Click **Choose File**, browse to the new language pack file, and click **Open**.
- 3 Click **Upgrade**.

To see the languages available in the installed language pack, click **View Supported Languages**.

Manage the RealPresence Web Suite Experience Portal User Roles

Users who attend meetings on the RealPresence Web Suite Experience Portal are assigned one of three roles: Chairperson, Participant, or Guest. Role assignment rules determine what role is assigned to an attendee when joining a meeting. The permissions that meeting attendees have are based on the role they have 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.



Note: Grayed out options

There are a few grayed out options displayed for each role and these options cannot be changed.

While a meeting is in progress, the Chairperson can change other user roles for that meeting.

Default User Permissions

The following table outlines the default permissions for each user role in RealPresence Web Suite meetings.

Default User 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.	✓		

Default User Permissions

Permission	A user with this permission can ...	Chairperson	Participant	Guest
Share Content	Share content with other meeting attendees.	✓	✓	
Invite Others	Invite additional users to attend the meeting.	✓		
Record	Start and stop a recording of the meeting and all presented content.	✓		
Promote	Assign a new role to a user, including promoting a participant to a chairperson or a guest to a participant or chairperson.	✓		
Roster Control	Mute or drop participants from the meeting roster. Add participants to the meeting (dial out).	✓		
Room Control	Dial out from an Multi-point Control Unit (MCU)-hosted VMR to a managed room endpoint at the user location or disconnect that endpoint from the VMR. This permission is only relevant if Polycom Concierge is available, but a personal device user is in a room with an endpoint that does not support Polycom Concierge (such as Polycom HDX). It enables the user to add that room endpoint to the meeting by having the MCU dial out to it. This permission is not needed for control of RealPresence Group Series endpoints that support Polycom Concierge and have been configured for direct control by a paired device.	✓	✓	

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 for RealPresence Web Suite Experience Portal meetings:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Conference > Roles Management > Permissions**.
- 2 Select the check boxes to add or remove permissions for **Participant** or **Guest** user roles.
- 3 Click **Apply**.
- 4 To return to the factory default permissions, click **Restore Default**.

Role Assignment Rules

Role assignment rules determine what role is assigned to an attendee when joining a meeting. The available role settings are chairperson, participant, guest, and disabled. If a rule is set to **Disabled**, the criterion described by that rule is not used to assign a role. Users who fit that rule are assigned a role based on one of the other rules, depending on how they were authenticated and how they joined the meeting.

The following table shows the default settings for the role assignment rules.

Default Role Assignment Rule Settings

Meeting Attendee	Attendee Definition	Role
Owner joins as	The owner of the VMR where the meeting is being hosted. This applies to meetings hosted on personal (static) VMRs assigned to an owner in the RealPresence® DMA® system.	Chairperson
Host joins as	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 join as	Users invited to the meeting by the host or by a participant whom the host has given permission to invite other users.	Participant
Users sharing owner domain join as	Users who are members of the Enterprise Directory domain to which the VMR owner belongs.	Participant
Users sharing host domain join as	Users who are members of the Enterprise Directory domain to which the host belongs.	Participant
First user joins as	The first user to join the meeting.	Disabled
Other authenticated users join as	Users who are authenticated with Enterprise Directory credentials, but are from a different domain than either the host or the VMR owner.	Participant
Unauthenticated users join as	Participants who have joined the meeting as a guest instead of as an authenticated user.	Guest

View and Change Roles Assignment Rules

You can change the role assignment rules applied to attendees when joining a meeting or reset them to the defaults as shown in the preceding table.

To view or change role assignment rules for RealPresence Web Suite Experience Portal meetings:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Conference > Roles Management > Roles Assignments**.
- 2 Select a different role setting for the role assignment rules you want to change.
- 3 Click **Apply**.
- 4 To return to the factory default rules, click **Restore Default**.

RealPresence Web Suite Experience Portal Platform Settings

This section provides information on configuring certain general platform settings for the RealPresence Web Suite Experience Portal. Platform settings enable the RealPresence Web Suite Experience Portal to communicate with the RealPresence Web Suite Services Portal and other components in the RealPresence Platform environment. They also enable users to host and attend meetings through the RealPresence Web Suite Experience Portal.

RealPresence Web Suite 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 Web Suite Experience Portal server (see [Upgrading the Portals](#)).

The following topics are included in this section:

- [Set the RealPresence Web Suite Experience Portal Date and Time](#)
- [Verify or Change the Network Configuration](#)
- [Generate Certificate](#)
- [Manage RealPresence Web Suite Experience Portal Logging](#)
- [Customize the User Interface](#)
- [Import the Application Data](#)
- [Activate License Information](#)
- [Restart the RealPresence Web Suite Experience Portal Services or Server](#)



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

If you make changes on a page, click **Apply** to save changes before moving to another page. If you open a new page without saving changes, the settings revert to the previously saved changes.

Set the RealPresence Web Suite Experience Portal Date and Time

The RealPresence Web Suite Experience Portal uses a Network Time Protocol (NTP) server for basic clock synchronization. In order for meetings to occur and for calls and recordings to work properly, both the RealPresence Web Suite Services Portal and the RealPresence Web Suite Experience Portal must reference the same time zone and NTP servers. The default time for instance is taken from the host server. If the time is incorrect, the RealPresence Web Suite Services Portal scheduler can go out of sync.

**Caution: Time must be synchronized among all RealPresence Platform products**

All your RealPresence Platform products, including RealPresence DMA, RealPresence Access Director, RealPresence Collaboration Server, the RealPresence Web Suite portals, and their hosts must use the same NTP servers so that time remains synchronized among them all.

If you set the time zone and NTP servers using console access after deployment, verify the time settings in the RealPresence Web Suite Experience Portal administration interface. Otherwise, set them there now.

To set the date and time on the RealPresence Web Suite Experience Portal:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Platform Settings > Date and Time**.
- 2 In the **NTP Server** field, enter a space-delimited list of time servers.
- 3 In the **Time Zone** list, select the proper time zone for the system.
- 4 Click **Update**.

The date and time for a particular time zone is set.

Verify or Change the Network Configuration

The network settings of both portals were configured during the installation process (see the *RealPresence Web Suite Getting Started Guide* at [Polycom Support](#)). You can verify or change the RealPresence Web Suite Experience Portal network configuration in its administration interface (for the RealPresence Web Suite Services Portal, this must be done in the restricted shell).

To verify or change the network configuration on the RealPresence Web Suite Experience Portal:

- 1 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Platform Settings > IP Configuration**.
- 2 Verify or change the IP address, subnet mask, and default gateway for the RealPresence Web Suite Experience Portal.
- 3 Verify or change the IP addresses of the Domain Name System (DNS) servers. The IP addresses for both Preferred and Alternate DNS servers are available. You may enter the IP addresses for both options. However, the Preferred DNS IP address is mandatory.
- 4 Alternatively, to enable Dynamic Host Configuration Protocol (DHCP) and disable the remaining fields, select **Obtain an IP address automatically**.
- 5 Click **Update**.

Generate Certificate

For more information on generating certificates, Certificate Signing Requests, and uploading certificates, see [Manage Certificates and Certificate Signing Requests](#).

Manage RealPresence Web Suite Experience Portal Logging

The RealPresence Web Suite 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. The more detail in a log, the more disk space required to store it, and the more system resources required to create it.

You can download all the log files on the portal as a compressed archive and view them or provide them to a Polycom Global Services representative to help resolve an issue.

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

RealPresence Web Suite Client software automatically writes log data to the browser console. You can configure the RealPresence Web Suite Experience Portal to collect these client console logs.

If Enhanced Content is enabled (see [Enhanced Content](#)), the RealPresence Web Suite Experience Portal also manages logging for the Standards Connectors. The logging level and disk usage threshold that you set in the RealPresence Web Suite Experience Portal also apply to the Standards Connectors. When you clear logs or download logs in the RealPresence Web Suite Experience Portal, the Standards Connector logs are included.

Set the Log Level

Logs are produced at the level of detail that you specify in Log Settings. The level of detail is greatest in Debug mode and least in Error mode. The system default is Info. When a log level is selected, all levels of less detailed logging are included in the information. For example, if you choose Info, the logs also include Error level information.

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.

The following table lists the log levels available on the RealPresence Web Suite Experience Portal.

Log levels, from most verbose to least verbose

Log Level	Description
Trace	Logs more detail than a Debug log. These logs are also helpful for debugging.
Debug	Logs fine-grained information that is helpful for debugging.
Info	Logs messages that highlight the progress of the application at a coarse-grained level.
Error	Logs errors that might cause the RealPresence Web Suite Experience Portal to stop running.



Note: For day-to-day operations, set the log level to Error or Info

Polycom recommends setting logging to **Error** or **Info** for day-to-day operations.

Debug logging produces highly detailed logs that require large amounts of disk space. While highly detailed logs are useful for troubleshooting a specific problem, we do not recommend Debug mode for day-to-day operations.

To set the log level on the RealPresence Web Suite Experience Portal (and if applicable, Standards Connectors):

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > Logs**.
- 3 Set **Level** to **Error**, **Info**, **Debug**, or **Trace** depending on the level of detail you want in your logs.



Note: The default log level is Info

By default, the log level is set to Info.

- 4 Set **Disk Usage Threshold (DUT)** to the maximum percentage of available disk space that can be used to store log files. The **Disk Usage Threshold (DUT)** is 80% by default.
When the log storage reaches the set threshold level, the system automatically begins deleting stored logs, with the oldest logs deleted first.
- 5 Optionally, turn on **Collect client logs**.
- 6 Click **Update**.
- 7 Navigate to **Platform Settings > Restart** and click **Restart Services** to implement the logging configuration changes.

Download and View Log Files

To help you troubleshoot problems, you can download all the log files on the portal as a compressed archive. A Polycom Global Services representative may request log files to assist in resolving an issue.

To download log files (including, if applicable, Standards Connector log files):

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > Logs**.
- 3 If necessary for troubleshooting or requested to do so by a Polycom Global Services representative, set **Level** to Debug to include more detail in your logs.
- 4 Click **Update** to begin logging at the selected level.
- 5 Navigate to **Platform Settings > Restart** and click **Restart Services** to implement the logging configuration changes. Then let the system run long enough to generate enough log information to help solve any issues that may be occurring.
- 6 Navigate to **Platform Settings > Logs**.
- 7 Set the start and end dates of the date range for which you want to download logs.

- 8 Click **Download**. When prompted to confirm, click **OK**.

A message informs you that the download is being prepared. Depending on the logging level and the date range you selected, this may take some time. Then the logs are saved to your Downloads folder as a compressed archive file.

Clear Log Files

You can clear all existing logs from the system.

To clear the log history in the RealPresence Web Suite Experience Portal and, if applicable, Standards Connectors:

- 1 Navigate to **Platform Settings > Logs**.
- 2 Click **Clear Logs** to remove all existing logs from the RealPresence Web Suite Experience Portal.

Customize the User Interface

For more information on customizing the user interface, see [Customize and White Label the User Interface](#).

On clicking **Refresh**, the settings from the RealPresence Web Suite Services Portal are retrieved and are applied to the RealPresence Web Suite Experience Portal.

Import the Application Data

Select the option **Migrate** under **Platform Settings** to migrate all the application data from the remote system to the current system.

For more information on migrating current settings to the new RealPresence Web Suite Experience Portal, see [Import Settings to the New RealPresence Web Suite Experience Portal](#).

Activate License Information

For more information on setting up and activating licenses, see [Activate Licenses](#).

Provide the information for the **License Server URL** and password credentials. On clicking **Apply**, the data from the RealPresence Web Suite Services Portal is retrieved and applied on RealPresence Web Suite Experience Portal. Click **Display License Info** to display the license details.

Restart the RealPresence Web Suite Experience Portal Services or Server

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

**Caution: Ensure there are no current users or calls**

Both restarting web services and rebooting the server will log out all users and end all calls. The system remains inaccessible until the server has rebooted and/or web services have restarted. Restart or reboot only during a maintenance window when there is no activity on the system.

Restart the RealPresence Web Suite Experience Portal Services

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

To restart all of the services related to the RealPresence Web Suite Experience Portal:

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > Restart**.
- 3 Click **Restart Services**, and in the confirmation dialog, click **OK**.
The services are stopped and restarted. All users are logged out, and all calls are ended.
- 4 Wait five minutes, and then log back into the administrator interface of the RealPresence Web Suite Experience Portal.

Reboot the RealPresence Web Suite Experience Portal Server

Rebooting the server shuts down and restarts the entire RealPresence Web Suite Experience Portal virtual server, logging out all current users and ending all current calls.

To reboot the RealPresence Web Suite Experience Portal server:

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Navigate to **Platform Settings > Restart**.
- 3 Click **Reboot Server**, and in the confirmation dialog, click **OK**.
The virtual server is stopped and restarted. All users are logged out, and all calls are ended.

Enhanced Content

RealPresence Web Suite Pro includes the Enhanced Content feature, which uses the capabilities of HTML5 content sharing to provide far greater content and collaboration functionality than the simple screen sharing otherwise available. Key Enhanced Content features include:

- Shared content can include documents uploaded to the meeting, whiteboards, and blackboards. Supported document types include PDF, PPT/PPTX, DOC/DOCX, and common image file formats.
- Multiple streams of content can be shared simultaneously, with the streams arranged locally to suit the available display capabilities.
- Multiple participants can share content simultaneously.
- Participants can annotate or edit their own or each other's content in real time and save the changes.
- Web browsers with native HTML5 support can participate directly. They share content with each other using HTML5 data distributed using the RealPresence Web Suite Experience Portal. Server-side media transcoding makes the shared content available to standards-based video endpoints.

Enhanced content sharing (uploading files, viewing and annotating shared documents, whiteboards, and blackboards) does not require a browser plug-in. HTML5 browsers require a plug-in or extension to share a screen or application, but not to view a screen or application shared by another participant.

If the Enhanced Content feature is not enabled (the default), RealPresence Web Suite users share content as H.264 video streams signaled through Session Initiation Protocol (SIP) and Binary Floor Control Protocol (BFCP), and distributed by an Multi-Point Control Unit (MCU).



Note: WebRTC clients do not support video-based (H.264) content sharing

RealPresence Web Suite clients using WebRTC are unable to share content unless Enhanced Content is enabled. For this reason, Enhanced Content must always be enabled when WebRTC is in use.

This section includes the following topics:

- [Configure the Enhanced Content Feature](#)
- [Add Standards Connector Servers](#)
- [Monitor Standards Connector Usage](#)

Configure the Enhanced Content Feature

To enable the sharing of content between HTML5 clients and standards-based clients, RealPresence Web Suite Pro uses the Standards Connector function. The Standards Connector provides a gateway function so that video-based content users can view enhanced content and vice-versa. It serves as a “two-headed” client that connects to RealPresence Web Suite conferences through HTTPS and video conferences hosted on the MCU using SIP, transcoding and adapting content between the two domains.

The RealPresence Web Suite Experience Portal server manages the Standards Connector function and monitors conferences to determine when Standards Connector functions are required. By default, it can use a built-in Standards Connector function to provide the content gateway function for a limited number of conferences. But we recommend deploying at least one dedicated Standards Connector server, as described in [Add Standards Connector Servers](#).

The following procedure describes how to configure the Enhanced Content feature. It assumes that the RealPresence Web Suite Pro license has been purchased and activated.



Note: Set conference template appropriately for Enhanced Content Service

To prevent Enhanced Content Service clients from receiving a redundant content view in their people video channel, the RealPresence DMA template used must have **Send content to legacy endpoints** turned off. Note, however, that this will prevent such legacy endpoints from receiving content.

For more information on properly setting up a conference template, see the *Polycom RealPresence DMA 7000 System Operations Guide* (available at [Polycom Support](#)).

To configure the Enhanced Content feature:

- 1 If SIP device authentication is enabled on the RealPresence DMA system (the recommended configuration), ensure that the SIP device authentication credentials have been specified in the RealPresence Web Suite Services Portal. See [Add a RealPresence DMA System and Access Points](#).

If device authentication is enabled, but the credentials are not specified in the RealPresence Web Suite Services Portal, Standards Connectors attempt to connect to the RealPresence DMA system as unauthenticated guests and are subject to the more restrictive guest dial plan.

- 2 In the RealPresence Web Suite Experience Portal administration interface, navigate to **Enhanced Content > Connector** and enter the correct password for the *ecsparticipant* system user.

The default password is *ecsparticipant*, which must be changed for security reasons. See [Required Internal System User Accounts](#).

- 3 Navigate to **Enhanced Content > Settings** and specify the file space and size limits for the Enhanced Content feature as described in the following table.

Setting	Description
Space per meeting	Select the maximum amount of file space per meeting for uploaded content. The default value is 50 MB.
File size	Select the maximum size file that can be uploaded. The default value is 10 MB.

- 4 To prevent meeting participants (including the chairperson) from being able to download files that have been uploaded to a meeting, select **Block files download**.
- 5 To send live drawing updates on the Whiteboard, enable the option **Send live update messages for pen tool**. If disabled, the live updates are visible only after the completion of the drawing.



Caution: Application performance

If this option is enabled, then this impacts the application performance.

- 6 Optionally, if many users have lower-resolution monitors (720, 768, or 800 pixels vertical resolution), navigate to **Enhanced Content > Resolution** and set **Content View Resolution** to **720p**. For most environments, leave the default setting of **1080p**.

This setting affects only full-screen sharing. At the default setting, when a lower-resolution monitor is being shared, participants with a higher-resolution monitor see a gray border around the shared content. Changing this setting to **720p** ensures that a screen shared from a lower-resolution monitor completely fills the content stage (no gray border) for all participants.

- 7 Click **Configure**.
- 8 Navigate to **Conference > General Settings**, select **Enhanced Content enabled**, and click **Apply**.
- 9 Navigate to **Platform Settings > Restart** and click **Reboot Server**.

Once Enhanced Content is enabled, you can monitor usage at **Enhanced Content > Connector**. Initially, the built-in Standards Connector (running on the RealPresence Web Suite Experience Portal server) is listed. We recommend that you maintain at least one dedicated Standards Connector instance for production deployments, and possibly more based on expected usage.

Add Standards Connector Servers

When you enable one or more dedicated Standards Connector servers, they are used in preference to the built-in Standards Connector function on the RealPresence Web Suite Experience Portal server. This provides for better scaling of that component and the overall solution. The RealPresence Web Suite Experience Portal built-in Standards Connector function remains available in the event that no more dedicated Standards Connector resources are available.

You can deploy as many Standards Connector servers as you need for the concurrent conference load you plan to support. They are not separately licensed. Refer to the latest *RealPresence Web Suite Release Notes* for information about host server and VM requirements and the number of concurrent conferences each Standards Connector server can support.

The RealPresence Web Suite Services Portal server does not communicate with the dedicated Standards Connector servers, which are managed by the RealPresence Web Suite Experience Portal.

The Standards Connector servers run the same software as the RealPresence Web Suite Experience Portal server and are deployed using the same file. They are simply configured differently.



Note: Co-locate RealPresence Web Suite Experience Portal and Standards Connector servers

The Standards Connector servers must be co-located with the RealPresence Web Suite Experience Portal that manages them, preferably in the same data center, and they must have a Gigabit Ethernet connection to the RealPresence Web Suite Experience Portal server.

The following procedure describes how to add dedicated Standards Connector servers. It assumes that the RealPresence Web Suite Pro license has been purchased and activated, and that the Enhanced Content feature has been enabled as described in [Configure the Enhanced Content Feature](#).

To add Standards Connector servers:

- 1 Obtain a static IP address for each Standards Connector server you want to deploy.

- 2 Deploy a new instance of RealPresence Web Suite Experience Portal software and configure its network settings as described in the *RealPresence Web Suite Getting Started Guide* (available at [Polycom Support](#)). This becomes a Standards Connector server.
- 3 In the administration interface of your RealPresence Web Suite Experience Portal, navigate to **Enhanced Content > Connector** and click **Add Connector**.
- 4 Under **Connector Instance Configuration**, complete the settings as described in the following table.

Setting	Description
Name	Enter a name for this Standards Connector.
IP Address	Enter the IP address for this Standards Connector.

- 5 Click **Configure**.
The RealPresence Web Suite Experience Portal connects to the connector instance and configures it as a Standards Connector.
- 6 Repeat the preceding steps for each additional Standards Connector server you want to deploy.
- 7 Navigate to **Platform Settings > Restart** and click **Reboot Server**.

Monitor Standards Connector Usage

You can monitor Standards Connector usage at **Enhanced Content > Connector**. If no dedicated Standards Connector server has been deployed, the built-in Standards Connector (running on the RealPresence Web Suite Experience Portal server) is listed. Otherwise, each dedicated Standards Connector server is also listed, and its status and capacity utilization are shown, as well as the total capacity and utilization. You can check this during periods of maximum conferencing activity to see if additional capacity is required.

The RealPresence Web Suite Experience Portal built-in Standards Connector function remains available in the event that no more dedicated Standards Connector resources are available. If you see that happening, you must deploy another dedicated Standards Connector server.

You can use the Standards Connector logs to help you monitor events and troubleshoot problems. Logging for the Standards Connectors is managed by the RealPresence Web Suite Experience Portal. The logging level and disk usage threshold that you set in the RealPresence Web Suite Experience Portal also apply to the Standards Connectors. When you clear logs or download logs in the RealPresence Web Suite Experience Portal, the Standards Connector logs are included. For more information on generating certificates, Certificate Signing Requests, and uploading certificates, see [Manage Certificates and Certificate Signing Requests](#).

RealPresence Web Suite Experience Portal Admin Management Menu

The **Admin Management** menu appears when you click the gear icon to the left of **Welcome user name** in the RealPresence Web Suite RealPresence Web Suite Experience Portal. It includes the following items:

- **Users Management** Lets you add and delete RealPresence Web Suite Experience Portal administrator accounts and change their passwords.
- **Server Management** Lets you change the ports used to access the RealPresence Web Suite Experience Portal administration interface.
- **Certificate Management** Lets you manage the certificate store specific to the RealPresence Web Suite Experience Portal administration interface.

The following topics are included in this section:

- [Manage RealPresence Web Suite Experience Portal Users](#)
- [Change RealPresence Web Suite Experience Portal Administration Ports](#)
- [Manage RealPresence Web Suite Experience Portal Administration Interface Certificates](#)

Manage RealPresence Web Suite Experience Portal Users

Users of the RealPresence Web Suite Experience Portal administration interface are the only RealPresence Web Suite users not managed in the RealPresence Web Suite Services Portal. RealPresence Web Suite Experience Portal administrators all have the Super Admin role. See [Account Roles](#).

The RealPresence Web Suite Experience Portal initially has one administrator with the user name *admin* and default password *Polycom12#\$*. At a minimum, you must change that password. For greater security, add individual administrator accounts for each authorized person and delete the generic *admin* account.

New RealPresence Web Suite Experience Portal administrator passwords must be at least eight characters and include the following:

- At least one upper case alpha character
- At least one lower case alpha character
- At least one numeric character



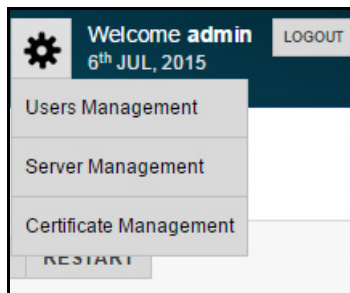
Caution: RealPresence Web Suite Experience Portal administrators are locked out after three failed login attempts

If an RealPresence Web Suite Experience Portal administrator attempts to log in with an incorrect password three times within an hour, the administrator account is locked for two hours.

Only Polycom Global Services can unlock the account before the lockout period is up.

To manage RealPresence Web Suite Experience Portal users:

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Click the gear icon to the left of the welcome message and select **Users Management** from the **Admin Management** menu, shown next.



The Administrators page appears.

- 3 To add a user, click **+ User**, enter the **Username** and **Password**, and click **Add**.
- 4 To delete a user, click the **✕** next to the account name. When prompted to confirm, click **Delete**.
A user who is currently logged in cannot be deleted.
- 5 To change a user password, click **!** next to the account, enter the new password in the dialog box, and click **Change**.

**Caution: Users are not notified of password changes**

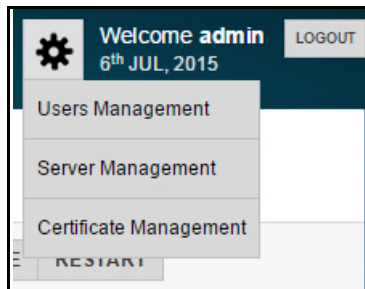
Unlike users maintained in the RealPresence Web Suite Services Portal, the RealPresence Web Suite Experience Portal administrators do not have an email address associated with their account and do not receive email notifications when their password changes. If you change someone else's password, you must notify them of the change.

Change RealPresence Web Suite Experience Portal Administration Ports

By default, the RealPresence Web Suite Experience Portal administration interface is securely accessed using port 9445. You can change this.

To change RealPresence Web Suite Experience Portal administration ports:

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Click the gear icon to the left of the welcome message and select **Server Management** from the **Admin Management** menu, shown next.



The Server Management page appears.

- 3 To use a different port for secure (https://) access, edit the **Secure Port** field.
- 4 To enable insecure (http://) access (not recommended), clear the **Secure Port** field, and if desired, edit the **Insecure Port** field.
- 5 Click **Apply**.
A message indicates that the configuration file has been updated and that you must reboot the server to apply the changes. Restarting services also applies the changes.
- 6 Navigate to **Platform Settings > Restart** and click **Restart Services** or **Reboot Server**. In the confirmation dialog, click **OK**.

Manage RealPresence Web Suite Experience Portal Administration Interface Certificates

The RealPresence Web Suite Experience Portal administration interface uses a different certificate store than its user interface. Super Admins can upload and view its certificates.

The certificate list and upload certificates functions are the same as those in **Platform Settings > Certificate** for the user interface certificate store. See [Manage Certificates and Certificate Signing Requests](#) for more detailed information about certificates.

No Certificate Signing Request (CSR)-generating function is available or necessary. Since the user interface and administration interface have the same Fully Qualified Domain Name (FQDN), you can use the same CSR you generated in **Platform Settings > Certificate** for the user interface or you can upload the same CA-provided certificates that you uploaded to the user interface certificate store.

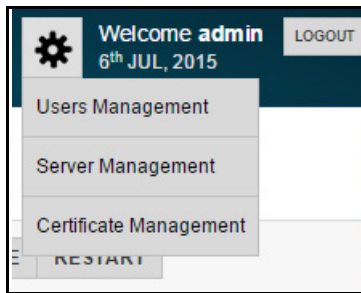


Caution: Select the right certificate type

When uploading a certificate, be sure to select the correct certificate type from the **Type** list to avoid possible server access problems.

To upload a certificate:

- 1 Log in to the administration interface of the RealPresence Web Suite Experience Portal with Super Admin credentials.
- 2 Click the gear icon to the left of the welcome message and select **Certificate Management** from the **Admin Management** menu, shown next.



The Certificate page appears.

- 3 Click **Upload Certificate**.
- 4 From the **Type** list, select the correct certificate type.
If you have a private key to upload, you must upload it first. To successfully install the public key certificate on a portal, the corresponding private key must already be present.
- 5 Click **Choose File** and select the certificate or certificate chain you want to upload.
- 6 Click **Upload**.
- 7 Navigate to **Platform Settings > Restart** and click **Restart Services** or **Reboot**.

Upgrading the Portals

Upgrading your RealPresence Web Suite system is accomplished by deploying a new version of each portal and migrating the configuration settings and data from the current version of each portal to the new version. The process is slightly different for each portal. The following sections describe the two processes.

- [Update RealPresence Web Suite Services Portal Software](#)
- [Update RealPresence Web Suite Experience Portal Software](#)

Update RealPresence Web Suite Services Portal Software

You can upgrade your RealPresence Web Suite Services Portal to a new version of the software by deploying a new instance of the portal and migrating the current configuration settings into the new portal.

Retrieve Current RealPresence Web Suite Services Portal Signed Certificate

You must copy the CA-signed webserver-own certificate from the current RealPresence Web Suite Services Portal so that you can upload it as a webserver-trust certificate to the new RealPresence Web Suite Services Portal later. This is necessary so that the new portal sees the current portal as a trusted server, allowing the data migration from the old portal to the new portal to take place.

To retrieve the current RealPresence Web Suite Services Portal certificate:

- 1 In the RealPresence Web Suite Services Portal administration interface, navigate to **Platform Settings > Certificate > Certificate List**.
- 2 Click **View** next to the webserver-own certificate.
- 3 Copy the entire certificate from **-----BEGIN CERTIFICATE-----** through **-----END CERTIFICATE-----** (include the leading and trailing dashes, but not anything preceding **-----BEGIN CERTIFICATE-----**).
- 4 Paste the text into a text editor.
- 5 Save the file with the file extension **.crt** and verify that the file appears as a certificate file in your file manager.

Deploy a New RealPresence Web Suite Services Portal with Upgraded Software

Before migrating the configuration settings, obtain the software for the new version you want to install, and deploy it in your virtual environment.



Note: Alternatively, use RealPresence® Platform Director to deploy the new portal

If you have RealPresence Platform Director in a vSphere® environment with the proper permissions, you can use it to create the new portal. Refer to the *RealPresence Platform Director Administrator Guide* (available at [Polycom Support](#)) for instructions.

To deploy a new RealPresence Web Suite Services Portal with upgraded software:

- 1 Obtain the new RealPresence Web Suite Services Portal Open Virtualization Archive (OVA) or Hyper-V® Export (*.zip) file from the Polycom Support site.
- 2 Deploy the new RealPresence Web Suite Services Portal in your virtual environment as described in the *RealPresence Web Suite Getting Started Guide* (available at [Polycom Support](#)).
- 3 Open the vSphere or Hyper-V Manager console for the new RealPresence Web Suite Services Portal VM.
- 4 Log in to the restricted shell using *polycom* as both your username and password. When prompted to do so, change the default password.

New passwords for the restricted shell users must include the following:

- At least 14 characters
 - At least one upper case character
 - At least one lower case character
 - At least one non-alphanumeric character
- 5 Enter `change_network_settings` and follow the prompts to assign a static IP address to the new portal.
Alternatively, if Dynamic Host Configuration Protocol (DHCP) is available, the new portal can temporarily use the IP address assigned to it through DHCP. After the old RealPresence Web Suite Services Portal is taken out of service, you can change this IP address to the old portal IP address.
 - 6 Enter `change_ntp` and follow the prompts to specify the same Network Time Protocol (NTP) servers as the old portal.
 - 7 Enter `change_timezone` and follow the prompts to specify the same time zone as the old portal.



Note: Time settings are also available in the administration interface of each portal

Instead of using the shell, you can view or change the NTP servers and time zone in each portal administration interface. In particular, choosing the time zone is easier in the administration interface of each portal. See [Set the RealPresence Web Suite Services Portal Date and Time](#) and [Set the RealPresence Web Suite Experience Portal Date and Time](#).

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

Migrate Current Settings to the New RealPresence Web Suite Services Portal

After deploying a new RealPresence Web Suite Services Portal running a new version of the software, you can use the migrate process to export settings from the old portal and import them into the new one.

**Note: Important steps to follow before migration**

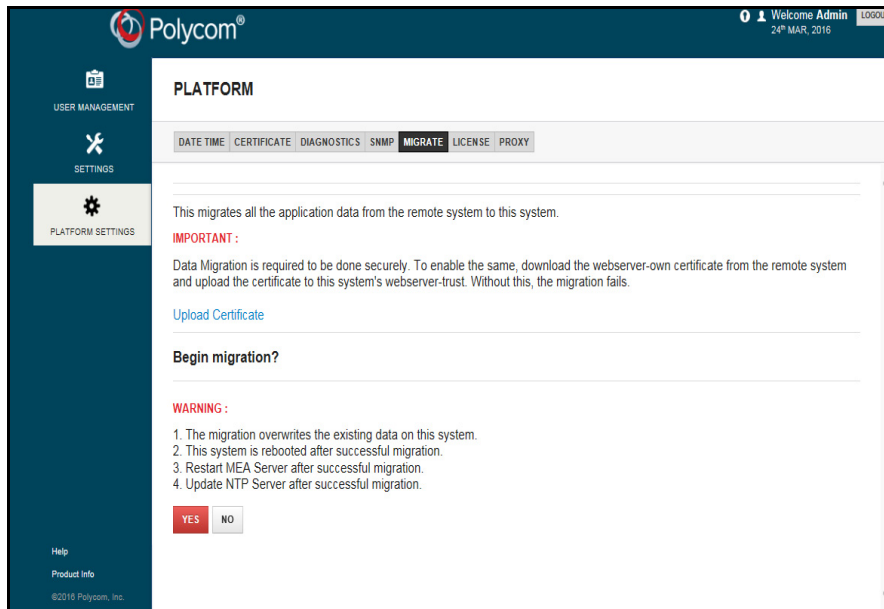
Before you begin the migrate process, be sure to complete the following important steps:

- Load the correct certificates on the new RealPresence Web Suite Services Portal to which you want to migrate the settings. See [Upload Certificates or a Certificate Chain](#).
- Deactivate the software licenses on the old portal. See [Deactivate Licenses](#). If there are any issues with deactivating the licenses, contact Polycom Global Services. If you have a RealPresence One™ solution subscription, license deactivation is not required.

To migrate current RealPresence Web Suite Services Portal settings to a new RealPresence Web Suite Services Portal:

- 1 Log in to the new RealPresence Web Suite Services Portal as the default administrator *admin* with password *Polycom12#\$*. When prompted, change the password and accept the license agreement.
- 2 Navigate to **Platform Settings > Certificate > Upload Certificate**.
- 3 From the **Type** list, select **WebServer Trust**.
- 4 Click **Browse**, navigate to the certificate that you retrieved from the old portal, and click **Upload**.
- 5 Navigate to **Platform Settings > Migrate**, and when prompted, enter your credentials.
- 6 Read the disclaimer on the **Platform Migration** page and click **Yes** when you are ready to begin the migration.
- 7 On the **Remote system details** page, enter the **Hostname** (Fully Qualified Domain Name (FQDN) or IP address), **Admin User Name**, and **Password** of the RealPresence Web Suite Services Portal from which you want to migrate the settings and database.
- 8 Click **Migrate**.
- 9 Wait for the user interface to indicate that the information from the old RealPresence Web Suite Services Portal was successfully imported.

After the data has been imported, additional configuration runs in the background before the RealPresence Web Suite Services Portal reboots. During these processes, the system displays progress information as follows.



Among the data imported from the old portal are its certificates and the user data, but not its network configuration.

- 10 After the new RealPresence Web Suite Services Portal has restarted, in your vSphere client or Hyper-V Manager, shut down the old RealPresence Web Suite Services Portal.

The old portal must be off when you assign its IP address to the new portal. After you confirm that the new portal is configured correctly, you can remove the old portal permanently at your convenience.

Change the Network Settings of the New RealPresence Web Suite Services Portal

Now that the new RealPresence Web Suite Services Portal has the configuration, data, and network settings of the old portal and the old portal has been shut down, you can configure the new portal to use the old portal IP address so that the old portal FQDN and certificates work for the new portal.

To change the new portal network settings:

- 1 Log in to the secure shell as user *polycom* with the password you created when you logged in to the shell after deployment.
- 2 Enter `change_network_settings`. If you previously assigned a temporary static IP address to the portal, you are prompted to enable DHCP if required. Enter `n`. The next prompt appears if you want to configure static network settings. Enter `y`.
- 3 Follow the prompts to make the IP address and other settings match those from the old portal.
- 4 After the new RealPresence Web Suite Services Portal has restarted, log in to its administration interface using the FQDN and Super Admin credentials **from the old RealPresence Web Suite Services Portal**.
- 5 Verify that the old portal certificate was successfully migrated and that your browser reports a secure connection (the address bar shows `https://` and a padlock icon is displayed).
- 6 Verify other aspects of configuration to satisfy yourself that the migration was successful.

**Note: A new IP address requires DNS record updates**

If you choose to assign a new IP address to the new RealPresence Web Suite Services Portal instead, update the DNS records to point to it.

Update RealPresence Web Suite Experience Portal Software

You can upgrade your RealPresence Web Suite Experience Portal to a new version of the software by deploying a new instance of the portal and migrating the current configuration settings into the new portal.

Export Current RealPresence Web Suite Experience Portal Settings

RealPresence Web Suite Experience Portal configuration settings are saved in its settings.json file. This file can be exported from the current RealPresence Web Suite Experience Portal server and imported into a new RealPresence Web Suite Experience Portal server. Do this first so that you can shut down the current RealPresence Web Suite Experience Portal; **it must be off** at later stages of the process.

To export the current RealPresence Web Suite Experience Portal configuration file:

- 1 In the administration interface of the current RealPresence Web Suite Experience Portal, navigate to **Platform Settings > Migrate**.
- 2 Enter your credentials.
- 3 Click **Export**.
The settings.json file is saved to the location you choose.
- 4 In your vSphere® client or Hyper-V® Manager, shut down the current RealPresence Web Suite Experience Portal.

Deploy a New RealPresence Web Suite Experience Portal with Upgraded Software

You can now deploy the new RealPresence Web Suite Experience Portal and configure its network and time settings to match those of the old RealPresence Web Suite Experience Portal. Before you do, **make sure that the old portal is shut down**. You can remove the old portal permanently at your convenience.

**Note: Alternatively, use RealPresence® Platform Director to deploy the new portal**

If you have RealPresence Platform Director in a vSphere® environment with the proper permissions, you can use it to create the new portal. Refer to the *RealPresence Platform Director Administrator Guide* (available at [Polycom Support](#)) for instructions.

To deploy a new RealPresence Web Suite Experience Portal with upgraded software:

- 1 Obtain the new RealPresence Web Suite Experience Portal OVA or Hyper-V® Export (*.zip) file from the Polycom Support site.
- 2 Deploy the new RealPresence Web Suite Experience Portal in your virtual environment as described in the *RealPresence Web Suite Getting Started Guide*.

- 3 Open the vSphere or Hyper-V Manager console for the RealPresence Web Suite Experience Portal Virtual Machine (VM).
- 4 Log in to the restricted shell using *polycom* as both your username and password. When prompted to do so, change the default password.
New passwords for the restricted shell users must include the following:
 - At least 14 characters
 - At least one upper case character
 - At least one lower case character
 - At least one non-alphanumeric character
- 5 Enter `change_network_settings` and follow the prompts to set its static IP address and other network settings to match those of the old portal.
- 6 Enter `change_ntp` and follow the prompts to specify the same NTP servers as the old portal.
- 7 Enter `change_timezone` and follow the prompts to specify the same time zone as the old portal.



Note: Time settings are also available in the administration interface of each portal

Instead of using the shell, you can view or change the NTP servers and time zone in each portal administration interface. In particular, choosing the time zone is easier in the administration interface of each portal. See [Set the RealPresence Web Suite Services Portal Date and Time](#) and [Set the RealPresence Web Suite Experience Portal Date and Time](#).

Import Settings to the New RealPresence Web Suite Experience Portal

The `settings.json` file that you exported from the old RealPresence Web Suite Experience Portal contains all of the configuration settings and data from the old portal. You can configure the new portal by importing that file.

To import the RealPresence Web Suite Experience Portal settings:

- 1 Log in to the new RealPresence Web Suite Experience Portal as the default administrator *admin* with password *Polycom12#\$*. When prompted, change the password and accept the license agreement.
- 2 Navigate to **Platform Settings > Migrate**.
- 3 Enter your credentials.
- 4 Under **Import Configuration**, click **Browse**, find the `settings.json` file that you exported from the old portal, and click **Open**.
- 5 Click **Import** to upload the settings and data.
- 6 Navigate to **Platform Settings > Restart** and click **Restart Services** to apply the changes and restart the RealPresence Web Suite Experience Portal and its administration interface.
- 7 After the new RealPresence Web Suite Experience Portal has restarted, log in to its administration interface using the FQDN and Super Admin credentials **from the old RealPresence Web Suite Experience Portal** and verify that the settings are correct.

**Note: Add password for ecsparticipant user if necessary**

If the settings.json file being imported is from a version prior to 2.0, it does not contain the new built-in system user, *ecsparticipant*. As a result, the password for *ecsparticipant* remains blank. Be sure to enter the password set for *ecsparticipant* in the RealPresence Web Suite Services Portal. The default is *ecsparticipant*, which must be changed for security reasons. See [Required Internal System User Accounts](#).

Deploy New Standards Connector Servers for Enhanced Content

If you are upgrading a RealPresence Web Suite Pro system with Enhanced Content enabled, you must also replace any existing Standards Connector servers with new ones deployed using the new RealPresence Web Suite Experience Portal OVA or Hyper-V® Export (*.zip) file. Remove the old Standards Connectors from your environment. Then follow the instructions in [Add Standards Connector Servers](#) to deploy the new versions.

Restricted Shell Commands

The RealPresence Web Suite restricted shell provides a means for you to log in to the RealPresence Web Suite portals from either a console or a Secure Shell (SSH) connection. You can connect to the RealPresence Web Suite Services Portal or RealPresence Web Suite Experience Portal shell through the vSphere® or Hyper-V® Manager console or with an SSH client, using the Fully Qualified Domain Name (FQDN) or IP address assigned to that portal.

The user accounts *caxis* and *polycom* are set up in the system to perform operations within the shell. These accounts have *caxis* and *polycom*, respectively, as their default passwords. You must change these passwords when you first connect to the shell.

New passwords for the restricted shell users must include the following:

- At least 14 characters
- At least one upper case character
- At least one lower case character
- At least one non-alphanumeric character

In addition, they must not be any of the following:

- Dictionary word or palindrome
- Previously used password
- Case change or rotated version of old password
- Too similar to old password (fewer than five characters changed)
- Too systematic (three or more sequential characters, such as def or 987, or repeated characters, such as aaa or ###).

The restricted shell supports basic Linux commands including `cat`, `ifconfig`, `ls`, `ping`, `grep`, `pwd`, `scp`, `tail`, `cd`, `echo` and `exit`. The restricted shell of the RealPresence Web Suite Experience Portal (but not the RealPresence Web Suite Services Portal) also supports the `openssl` command.

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

Restricted Shell Operations

Operation	Shell Command	Notes
View status of web services	<code>service nginx status</code> <code>service rpp-tomcat status</code>	Show status for nginx and Tomcat. When these services are not running, users cannot access the web portals.
Start web services	<code>service nginx start</code> <code>service rpp-tomcat start</code>	Start services that are not running. Do not use to restart services that are running.

Restricted Shell Operations (continued)

Operation	Shell Command	Notes
Restart web services	<pre>service nginx restart service rpp-tomcat restart</pre>	Restart web services that are running. Note: This can be done in the administration interface of the RealPresence Web Suite Experience Portal. Caution: Both restarting web services and rebooting the server will log out all users and (for the RealPresence Web Suite Experience Portal) end all calls. The system remains inaccessible until the server has rebooted and/or web services have restarted. Restart or reboot only during a maintenance window when there is no activity on the system.
Collect log files	<code>collect_logs</code>	Collect all the log files on a server into an archive file. You can use the <code>scp</code> command to securely copy that file to another location.
Change system host name	<code>change_hostname</code>	Displays the current host name, along with a prompt asking whether you want to change the host name. Type the new host name exactly as specified in Domain Name System (DNS). A confirmation message is displayed for the name changed successfully.
Change the password for the caxis or polycom user	<code>passwd</code>	Change the password for the shell user account with which you are logged in. New shell user passwords must meet the requirements specified prior to this table.
Configure or change Network Time Protocol (NTP) settings	<code>change_ntp</code>	Displays a list of NTP servers configured in the system. Follow the prompts to add new time servers. Note: This can be done in the administration interface of each portal.
Synchronize system date and time with a specific NTP server	<code>ntpdate -u <FQDN or IP address of the NTP server></code>	The system indicates that the time has been adjusted.

Restricted Shell Operations (continued)

Operation	Shell Command	Notes
Set or change system date and time	change_system_datetime	Follow the prompts, and then enter the date and time in the following format: <i>Day Month Date Hour:Minute:Second Zone Year</i> For example: Mon Jun 17 20:27:27 UTC 2015 The system indicates when a time and date change has been successful. Note: Setting the date and time manually is appropriate only to get the system time close to the NTP server time to which it must be synchronized.
Change the time zone for the system	change_timezone	The current time zone is displayed. Follow the prompts to change the time zone, pressing ENTER repeatedly to scroll through a list of 608 time zones from which to choose, and finally entering the number of that time zone at the prompt that appears at the end of the list. Note: Choosing the time zone is easier in the administration interface of each portal. See Set the RealPresence Web Suite Services Portal Date and Time and Set the RealPresence Web Suite Experience Portal Date and Time.
View system network information	show_network_info	Displays all relevant network settings, including IP configuration and the DNS domain and servers.
Change network settings	change_network_settings	Lets you make the following network setting changes: • Enable or disable Dynamic Host Configuration Protocol (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.
View system space information	show_system_info	Displays all relevant space information for each file system, including total space, used space, available space, used percentage, and mounted directory.

Restricted Shell Operations (continued)

Operation	Shell Command	Notes
Reboot the server	reboot	Stops and restarts the server. Caution: Both restarting web services and rebooting the server will log out all users and (for the RealPresence Web Suite Experience Portal) end all calls. The system remains inaccessible until the server has rebooted and/or web services have restarted. Restart or reboot only during a maintenance window when there is no activity on the system.
Show the current product version	show_product_info	Displays the version or build number of the RealPresence Web Suite Services Portal or RealPresence Web Suite Experience Portal software.
Regenerate self-signed certificate	regenerate_certificates	Creates a new self-signed certificate, replacing the current one. A message indicates that the certificate has been regenerated successfully. Follow the prompts to restart the web services and apply the new certificate. Note: For the RealPresence Web Suite Services Portal, this can be done in the administration interface. But Polycom strongly recommends using trusted CA-signed certificates. Caution: Both restarting web services and rebooting the server will log out all users and (for the RealPresence Web Suite Experience Portal) end all calls. The system remains inaccessible until the server has rebooted and/or web services have restarted. Restart or reboot only during a maintenance window when there is no activity on the system.
Manage RealPresence Web Suite Services Portal features	manage_feature	RealPresence Web Suite Services Portal only. Enable or disable features. Currently, the command controls only one feature, SS0_WITH_SAML, which is not yet fully implemented and is not supported.
Manage firewall	firewall	RealPresence Web Suite Services Portal only. Lets you check the current status of the firewall and activate or deactivate it.

Recommendations for Secure Access

The section provides information on providing invited guests and remote users with controlled access to your organizational unified communications infrastructure while preventing unwelcome intrusion.

This section includes the following topics:

- [Secure Web Access](#)
- [Tunnel Access for Remote Users](#)
- [Secure SIP Access for Guests](#)

Secure Web Access

To provide conference access to guest users joining from outside your organizational firewall, they must be able to access the RealPresence Web Suite Experience Portal from the Internet. Access to the RealPresence Web Suite 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 Web Suite Services Portal component is left to the administrator 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 Web Suite Experience Portal to its internal IP address. Do the same for the RealPresence Web Suite Services Portal if desired.
- Use a reverse proxy product to provide external HTTPS access to the RealPresence Web Suite Experience Portal. Do the same for the RealPresence Web Suite Services Portal if desired.

The proxy selected must 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.example.com` and `schedule.example.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™ product, version 3.0 or later, can be configured to perform this function. For more information, see the “Configure Access Proxy Settings” section of the *Polycom RealPresence Access Director System Administrator Guide* (available at [Polycom Support](#)).

Tunnel Access for Remote Users

Restrictive firewall policies on remote networks may block egress for User Datagram Protocol (UDP)-based traffic, limit Transmission Control Protocol (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 in the RealPresence Web Suite Services Portal (see [Configure RealPresence DMA and Access Points](#)). 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.
- Scalable Video Coding (SVC) calls are not supported over HTTP tunnels. If a RealPresence Web Suite 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 Web Suite 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 Web 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 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 Web Suite is aware of the web proxy through the web browser configuration, the RealPresence Web Suite plug-in can participate in this authentication process.
 - In the case of transparent web proxies, where RealPresence Web Suite is not aware of the web proxy through the web browser configuration, the RealPresence Web 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 documentation or support for possible workarounds to this problem.
- If the RealPresence Web Suite solution is configured to support tunneled calls, the RealPresence DMA system configuration must allow Session Initiation Protocol (SIP) UDP connections for internal users. This is necessary in order to support the RealPresence Web Suite browser client detection of whether or not tunneled calls are required. Failure to ensure this results in unnecessary tunneled calls for internal users. Note that RealPresence Web Suite uses TLS for SIP connections.

Refer to “Working with Access Proxy Settings” in the *Polycom RealPresence Access Director System Administrator Guide* (available at [Polycom Support](#)) for more information.



Note: Certificates for HTTPS Proxy with the RealPresence Web Suite Experience Portal

If you add host-header next hops, you must specify the host Fully Qualified Domain Names (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 Web Suite web client functions by default in a guest mode; it neither registers nor authenticates itself with your organizational 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, the RealPresence Mobile software endpoint for mobile devices, 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 Web Suite Experience Portal.

You can enable authenticated SIP access for verified members of your organization by enabling SIP device authentication on the RealPresence DMA system and configuring the SIP username and password information in the RealPresence Web Suite Services Portal DMA settings (see [Configure RealPresence DMA and Access Points](#)). These credentials are automatically and securely provided to supported endpoints for the members of your organization who have authenticated to the RealPresence Web Suite Services Portal. Supported endpoints include the RealPresence Web Suite client (plug-in) and Polycom RealPresence Mobile v3.1 and later, 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, as recommended in a following section.

Guest users who have not authenticated to the RealPresence Web Suite Services Portal are not provided the SIP credentials. They are instead always dialed in as unauthenticated SIP callers subject to the RealPresence DMA system dial rules for unauthenticated endpoints.

In order for guest (unauthenticated) callers to join a conference, the RealPresence DMA system must have at least one dial rule for unauthenticated access that handles calls to the access point to which these callers are directed. This dial rule must have the action **Resolve to conference room ID**. For more information about dial rules and preliminary scripts on the RealPresence DMA system, see the *Polycom RealPresence DMA 7000 System Operations Guide* (available at [Polycom Support](#)).

Edge Proxy Access for Guests

To enable guest access across your organizational edge proxy device, refer to one of the following Polycom publications. Follow the recommendations for enabling endpoint authentication on the applicable RealPresence DMA system as described in the following 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* (available at [Polycom Support](#)).
- See “Deploying the Polycom—Acme Packet Solution to Support Remote and Guest Users” in *Deploying Polycom Unified Communications in an Acme Packet Environment* (available at [Polycom Support](#)).

Edge proxies, including the RealPresence Access Director, may require authenticating and non-authenticating callers to distinguish themselves by sending SIP requests to a different port or by using a special dialing prefix. To facilitate such a configuration, specify the correct Authentication Mode when configuring access points in the RealPresence Web Suite Services Portal configuration (see [Configure RealPresence DMA and Access Points](#)). 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 video conferencing infrastructure:

- Use temporary rather than persistent static (personal) Virtual Meeting Rooms (VMRs) for meetings that include untrusted guests. Using temporary VMRs helps ensure that guests are able to access only the specific conference session to which they are invited.

In **Settings > Conference Settings**, the default **Personal VMR** setting is **Do not allow users to schedule meeting on Personal VMR**, which disables the **Use Personal VMR** option on the **Schedule a Meeting** page. See [Configure Conference Settings](#). Alternatively, you can instruct your users not to select **Use Personal VMR** on the **Schedule a Meeting** page for meetings that include untrusted guests. See the *Polycom RealPresence Web Suite User Guide* for more information.

- Select the **Require Authentication** check box on the **Schedule a Meeting** page to provide an additional level of access control.
- Select the **Generate VMR from Range** check box in **Settings > DMA Config** to generate random temporary conferencing IDs in a wide range. This makes the IDs more difficult to access by random dialing. See [Configure RealPresence DMA and Access Points](#).
- 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 specific 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 100000 to 999999, which could be configured to be the same auto-generation range used by the RealPresence Web Suite Services Portal to create temporary VMRs.

```
// These values should correspond to the min and max room ID settings
// specified in the RealPresence Web Suite Services Portal DMA Config
// Option "Generate VMR From Range"
var minGeneratedRoomId = 100000;
var maxGeneratedRoomId = 999999;
var number = parseInt(DIAL_STRING.replace(/^sipL[^\@]*\)?@?(.*)/I,"$1"));
if (NaN != number && number > minGeneratedRoomId && number < maxGeneratedRoomId){
    return;
}
return NEXT_RULE;
```

For more information about dial rules and preliminary scripts on the RealPresence DMA system, see the *Polycom RealPresence DMA 7000 System Operations Guide* (available at [Polycom Support](#)).

Troubleshooting

This section describes how to troubleshoot and resolve certain issues with RealPresence Web Suite. For information about logging levels and obtaining the log files from each server, see [Manage RealPresence Web Suite Services Portal Logging and Data Collection](#) and [Manage RealPresence Web Suite Experience Portal Logging](#).

For more information on generating certificates, Certificate Signing Requests, and uploading certificates, see [Manage Certificates and Certificate Signing Requests](#).

This section includes the following troubleshooting topics:

- [Portal URL \(FQDN\) is unresponsive](#)
- [RealPresence Web Suite Experience Portal fails to connect to RealPresence Web Suite Services Portal and get licensing information](#)
- [User cannot create meetings](#)
- [User cannot start a meeting using Meet Now function in RealPresence Web Suite Services Portal](#)
- [User cannot launch the Welcome screen](#)
- [Chrome user cannot join meeting with audio or video](#)
- [Configured components do not respond](#)
- [Super Admins and Admins cannot add Enterprise Directory users](#)
- [User cannot send email notifications](#)
- [User receives message: "Unable to create a conference with a personal VMR"](#)
- [User receives message: "External server not set"](#)
- [User receives message: "Resources are not available"](#)
- [Enhanced Content users have trouble viewing shared content or see content updates only after long delays](#)
- [Users of Enhanced Content cannot see content shared from standards-based endpoints or vice versa](#)
- [WebRTC guest callers receive message: "No such VMR"](#)
- [Remote WebRTC callers fail to connect or are disconnected when a mesh meeting is transitioned to a Multi-point Control Unit \(MCU\)](#)
- [Administrator cannot download log files with Internet Explorer](#)
- [User cannot see all participants in the Roster](#)
- [Single Sign-On \(SSO\) is not working](#)
- [SSO authentication has failed](#)

Portal URL (FQDN) is unresponsive

To enable browser access to the RealPresence Web Suite portals, the nginx and Apache Tomcat services must be running on the servers. Unresponsive web addresses can indicate that those services are not running. If a portal URL does not respond when you attempt to open it in a web browser, log in to its restricted shell and confirm that the nginx and rpp-tomcat services are running. Start or restart them if necessary. The shell commands for doing so are described in [Restricted Shell Commands](#).

If the problem persists and you need to collect logs, use the shell `collect_logs` command.

RealPresence Web Suite Experience Portal fails to connect to RealPresence Web Suite Services Portal and get licensing information

If the RealPresence Web Suite Experience Portal fails to connect to the RealPresence Web Suite Services Portal as its license server (see [Set Up Licensing for the RealPresence Web Suite Experience Portal](#) or [Activate the RealPresence Web Suite Experience Portal License Server Connection](#), depending on how licensing is managed), do the following:

- Complete all RealPresence Web Suite Experience Portal configuration and try again.
- Confirm that the passwords for the built-in system users *meaconf*, *meaauth*, and *measys* are correct.

For security reasons, you must change the default passwords for these users (which are the same as the user names). Log in to the RealPresence Web Suite Services Portal as these users to verify that you are using the correct passwords.

User cannot create meetings

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

- At least one RealPresence DMA system connection is set up.
- The connected RealPresence DMA system status is up.
- The **Owner Username** entered in the RealPresence Web Suite Services Portal for the RealPresence DMA system also exists in the RealPresence DMA system (see [Add a RealPresence DMA System and Access Points](#)).

For information on how to create a user ID for the RealPresence DMA system, see the *Polycom RealPresence DMA 7000 System Operations Guide* (available at [Polycom Support](#)).

User cannot start a meeting using Meet Now function in RealPresence Web Suite Services Portal

If users who select Meet Now in the RealPresence Web Suite Services Portal are not redirected to the RealPresence Web Suite Experience Portal, this could be a trust-related issue due to self-signed certificates, especially in a non-split-Domain Name System (DNS) scenario with the RealPresence Access Director system acting as reverse proxy.

Polycom strongly recommends using trusted Certificate Authority (CA)-signed certificates for the RealPresence Web Suite portals and for all other components of the RealPresence Platform solution, including the RealPresence Access Director system.

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 Web Suite Experience Portal (see [Configure the RealPresence DMA Agent](#)).

Chrome user cannot join meeting with audio or video

The Chrome browser requires hardware acceleration in order to display meeting video. If it is not available, the user sees an error message stating “Cannot join the meeting with Audio/Video” when attempting to join. The message tells the user how to enable hardware acceleration and advises contacting the system administrator or using a different browser if it does not work. If assisting the user, check the following on the user PC:

- In the Chrome address bar, enter `chrome://settings`. In the search box, type hardware. Verify that **Use hardware acceleration when available** is selected.
- In the Chrome address bar, enter `chrome://gpu`. If, under **Graphics Feature Status**, the entry for Canvas states “Software only. Hardware acceleration unavailable,” the user PC requires updated graphics drivers.

Configured components do not respond

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

Super Admins and Admins cannot add Enterprise Directory users

If the RealPresence Web Suite Services Portal Admin and Super Admin users are unable to add an Enterprise Directory user, confirm that the proper Lightweight Directory Access Protocol (LDAP) server is configured with the correct values (see [Set Up LDAP Authentication](#)).

User cannot send email notifications

If users are unable to send email notifications, confirm the following (see [Enable Email Notifications for Users](#)):

- The proper Simple Mail Transfer Protocol (SMTP) server is configured with the correct port numbers.
- If a secure connection is required, the service account user credentials are correct.
- If the SMTP server is configured to reject messages from senders who are not authenticated users, the sender mail ID is white-listed.

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

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

In the RealPresence Web Suite Services Portal, confirm that the **Default Admin** specified for the connected RealPresence DMA system is an Enterprise Directory administrator on the RealPresence DMA system (see [Add a RealPresence DMA System and Access Points](#)). A local administrator cannot see Enterprise Directory users.

Confirm that the virtual meeting room exists on the connected RealPresence DMA system. If it exists, contact Polycom Global Services.

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 the RealPresence Web Suite Services Portal **Server Settings** page (see [Set Web Addresses for the Portals](#)).

User receives message: “Resources are not available”

This error message appears 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 Web Suite system or to increase your user capacity.

Enhanced Content users have trouble viewing shared content or see content updates only after long delays

Check the performance and bandwidth of the network connection between the sharing user and the RealPresence Web Suite Experience Portal server and between the viewing users and the RealPresence Web Suite Experience Portal server.

Note that unlike standards-based content, Enhanced Content does not flow through the RealPresence Collaboration Server. Therefore, content sharing statistics reported by the RMX Manager administration utility do not reflect content sharing between Enhanced Content users. When the Standards Connector is in operation to bridge content between the HTML5 and standards-based content domains, however, those content flows are reflected in RMX Manager statistics.

Users of Enhanced Content cannot see content shared from standards-based endpoints or vice versa

This is generally due to a problem with the Standards Connector. Check the Standards Connector configuration and status in the RealPresence Web Suite Experience Portal administration interface. It may be necessary to restart the Standards Connector servers or the RealPresence Web Suite Experience Portal server in order to resolve this problem.

WebRTC guest callers receive message: “No such VMR”

In the RealPresence DMA system, navigate to **Admin > Call Server > Dial Rules** and make sure there is a dial rule for unauthorized calls with the action set to **Resolve to conference room ID**. See [Enable WebRTC Support in the RealPresence DMA System](#).

Remote WebRTC callers fail to connect or are disconnected when a mesh meeting is transitioned to a Multi-point Control Unit (MCU)

In addition to a network problem, this can be due to incorrect Traversal Using Relays around NAT (TURN) server configuration. Specifically, it happens if:

- The Session Traversal Utilities for NAT (STUN) or TURN server address specified in the RealPresence Web Suite Experience Portal WebRTC agent settings is incorrect.
- The TURN user credentials specified in the RealPresence Web Suite Experience Portal WebRTC agent settings are invalid.
- The STUN or TURN server is down or is unreachable by the remote client.

See [Enable WebRTC Support in the RealPresence Web Suite Pro System](#).

Administrator cannot download log files with Internet Explorer

Follow the steps provided on the user interface and retry downloading the logs. Or try using a different browser.

User cannot see all participants in the Roster

Verify that the dial prefixes for the RealPresence DMA system are the same on the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal, and verify that the RealPresence DMA system password configured on the RealPresence Web Suite Experience Portal is correct.

Single Sign-On (SSO) is not working

The following table lists reasons why SSO may not be working properly for a user with possible solutions for each.

SSO Issues and Solutions

Problem	Solution
RealPresence Web Suite could not obtain a Kerberos ticket from the domain. This can happen if the domain is temporarily unavailable. For example, it may occur when the user is connected to the network through VPN or on a laptop with multiple network interfaces that do not include the correct Windows domain.	Check 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 account (the RealPresence Web Suite Services Portal user), and RealPresence Web Suite resorts 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 RealPresence Web Suite Services Portal User Account in Enterprise Directory .
The HTTP service account (the RealPresence Web Suite Services Portal user) is disabled.	In Enterprise Directory, check the RealPresence Web Suite Services Portal user account and enable it.
If the user enters credentials into the Network Password dialog box, the browser will continue to submit network credentials using NTLM authentication even after the issue with the user network password has been resolved.	Purge saved passwords. Navigate to 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 on the servers is not synchronized.	Synchronize the time on the servers using an Network Time Protocol (NTP) server (see Set the RealPresence Web Suite Services Portal Date and Time and Set the RealPresence Web Suite Experience Portal Date and Time) and check the times regularly.

SSO authentication has failed

The SSO authentication feature in the RealPresence Web Suite Services Portal is provided by a separate bundle in a **war** package. When SSO authentication fails, a set of error and debug messages is written to the log file `/var/log/polycom/rpp-tomcat/cloudaxis_wsp-ui.log`. To troubleshoot SSO authentication issues, set the log level to Debug to capture the debug messages (see [Set the Log Level](#)). In the log file, look for debug messages with the log patterns that follow. An explanation follows each debug message type.

Debug Message Type 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

Explanation:

These errors indicate one of the following:

- DES security is needed, but the domain user account does not have **Use DES Encryption types for this account** selected.
- RC4-HMAC security is needed, but the domain user account does have **Use DES Encryption types for this account** selected.
- The wrong keytab utility was used to generate the keytab file. For example, the Sun keytab utility was used on a WebSphere system. See [Generate a Keytab File for the RealPresence Web Suite Services Portal User](#) for information on generating a keytab file.

Debug Message Type 2

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

Explanation:

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

- **Duplicate Service Principal Names (SPNs)** SPNs must 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, a user must initiate their login within the domain. If a user has not logged in to the domain before starting SSO authentication, they would not 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 fall back to using NTLM.
- **Incorrect Browser Configuration** The browser must be configured to trust the target server to send the credentials. In Internet Explorer, the user must add the target server or its domain under **Tools > Internet Options > Security > Intranet Zone**. Make sure it is Intranet Zone. In some browsers, Integrated Windows Authentication must also be turned on to enable automatic authentication. In Internet Explorer, click **Tools > Internet Options > Advanced** and select **Enable Integrated Windows Authentication**.
- **Outdated Windows Login** After the SPN has been set or changed, 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 that users log out and log back into the AD domain.
- **Outdated Saved Network Credentials** If a user entered credentials into a Network Password dialog box and elected to save them, the client uses those credentials, initiating NTLM rather than Kerberos.

- **SPN in general** If there is a problem with the SPN on the service account or domain user account that prevents the client from initiating Kerberos authentication, the client has no choice but to fall back to using NTLM.
- **DNS host name** Make sure the RealPresence Web Suite Services Portal URL host name is a DNS A record host name, not a CNAME alias. When the browser requests a ticket from KDC, it always uses the DNS A record host name, regardless of the host name that appears in the browser address bar. Users can still use CNAME alias host names to access the site, but the keytab file must be created using an A record host name.

Debug Message 3

```
org.ietf.jgss.GSSEException: 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 [Set the RealPresence Web Suite Services Portal Date and Time](#) and [Set the RealPresence Web Suite Experience Portal Date and Time](#)).

Appendix 1: Deploy the WebRTC Solution

RealPresence Web Suite Pro can be configured to support Web Real-Time Communication (WebRTC), but the WebRTC solution depends on proper configuration of multiple RealPresence® Platform components. Enabling WebRTC in RealPresence Web Suite Pro is the final step in the solution deployment process. The following sections describe WebRTC, the components required for the WebRTC solution, and the deployment of the solution:

- [Overview of WebRTC](#)
- [Polycom WebRTC Solution Components](#)
- [Implementing the WebRTC Solution](#)

Overview of WebRTC

WebRTC is a web-based real time communication technology that provides high-quality video and audio communications capabilities in WebRTC-capable browsers such as Google Chrome without requiring installation of a custom plug-in. The RealPresence Platform WebRTC solution supports conferencing between WebRTC clients and other clients and endpoints.

In a Polycom WebRTC deployment, the following conferencing scenarios are supported:

- WebRTC clients participating in mesh meetings (see [Mesh Conference Mode](#)), where media is exchanged directly between endpoints without using Multi-point Control Unit (MCU) resources.
- WebRTC, SIP, H.323, Lync, and other clients connected together in bridge-based conferences where media are exchanged through an MCU or conferencing bridge.
- Automatic transition from a mesh meeting to a bridge conference to accommodate different conferencing scenarios, including conferences with non-WebRTC-capable endpoints.

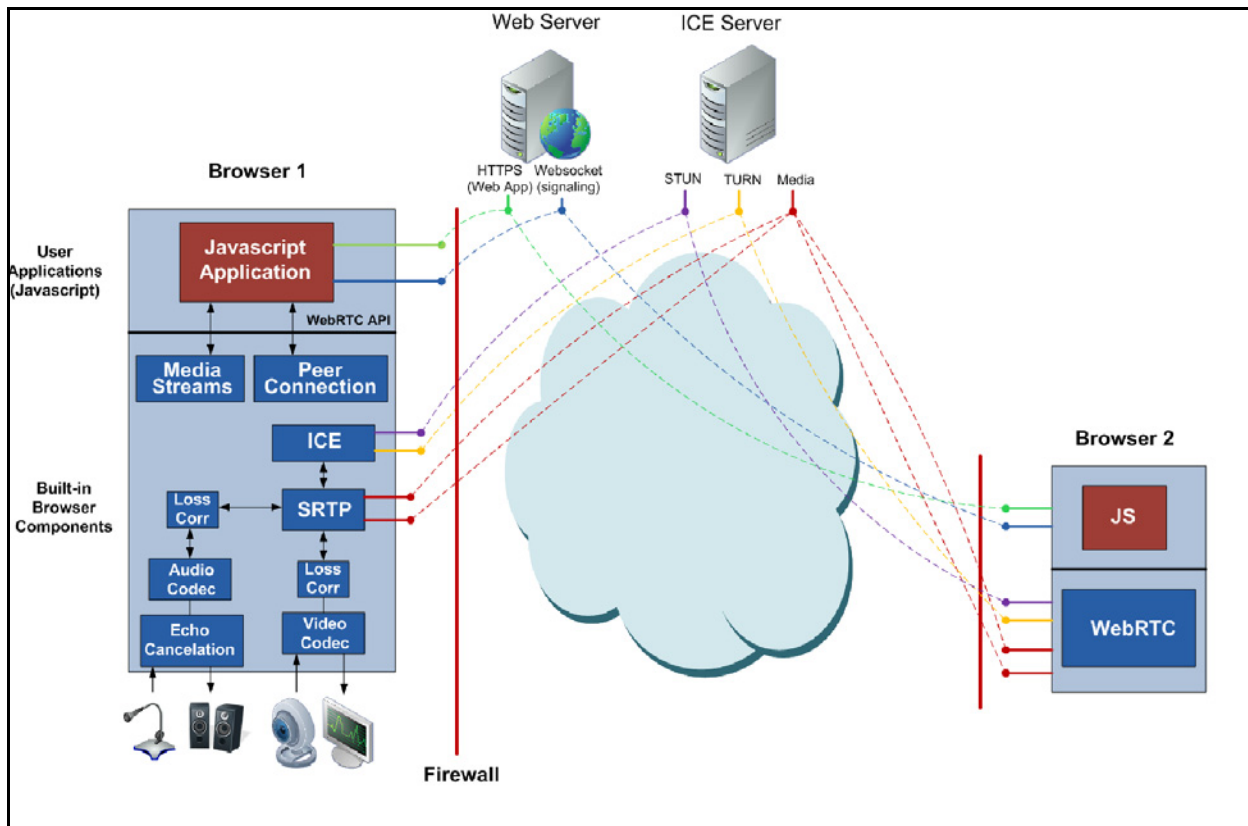
WebRTC includes the following architectural components:

- **JavaScript Application** WebRTC applications include a mix of HTML5 and JavaScript, which can theoretically be supported on any WebRTC-enabled web browser on any operating system.
- **WebRTC APIs** The JavaScript application functions in a WebRTC-enabled browser and uses standard WebRTC APIs to establish RTC sessions with other WebRTC clients. WebRTC APIs are supported within supporting web browsers without the need for plug-ins.
- **WebRTC Browser Native Stack** A WebRTC-enabled browser supports a stack of software components required for high-quality RTC user experiences, including audio and video codecs, key media processing functions such as echo cancellation and packet loss correction, media encryption for secure transport, and ICE support for facilitating media exchange between WebRTC peers.
- **WebRTC Application Server** A WebRTC-enabled web server downloads the JavaScript application to web clients and provides a point of centralized access and control for the application as well as a “meeting point” for WebRTC clients to discover and connect to one another.

- Signaling Framework** WebRTC does not mandate a specific signaling protocol like Session Initiation Protocol (SIP) or H.323. Instead, it specifies the JavaScript Session Protocol (JSEP), which defines the methods for creating, manipulating, and exchanging Session Description Protocol (SDP) offers and answers over a signaling transport to be determined and provided by a specific vendor WebRTC implementation. Like most vendor implementations, the Polycom WebRTC solution leverages a WebSocket-based transport framework for signaling.
- ICE Services** Provides for media connectivity between WebRTC clients in different Network Address Translation (NAT) and firewall domains using the standard Session Traversal Utilities for NAT (STUN) and Traversal Using Relays around NAT (TURN) protocols.
- Interoperation with Other Communication Platforms** Some WebRTC architectures provide network gateways to support interoperability between WebRTC endpoints and other endpoints not natively enabled for WebRTC. Polycom RealPresence Collaboration Server, Virtual Edition, implements WebRTC media capabilities natively to provide “meet-on-the-bridge” WebRTC media interoperability with non-WebRTC endpoints. The RealPresence DMA system provides WebRTC signaling interoperability by translating WebRTC signaling to SIP where and when necessary.

The following figure illustrates a very simple WebRTC architecture where the internal components of WebRTC-enabled browsers on two endpoints rely on servers in their environment to deliver the application and establish a peer-to-peer RTC session.

Simple WebRTC Call Model



The following table compares the handling of various functions in Session Initiation Protocol (SIP), H.323, and WebRTC.

WebRTC Comparison

Function	SIP World	H.323 World	WebRTC World
Signaling Protocol	SIP	H.323	JSEP with proprietary messaging and signaling
Media Transport	Real-time Transport Protocol (RTP) – separate streams for each media session	RTP – separate streams for each media session	RTP – all media multiplexed over a single session and User Datagram Protocol (UDP) port
Video Codecs	H.264, H.263, others	H.264, H.263, others	VP8
Audio Codecs	Siren, G.729, G.711, others	Siren, G.729, G.711, others	OPUS, G.711
Media Encryption	Secure Real-time Transport Protocol (SRTP) – with SDP key exchange	SRTP – with SDP key exchange	SRTP – with DTLS key exchange
NAT/FW Traversal	SBC	H.460	ICE/STUN/TURN
Content Format	Video	Video	HTML5 (Polycom)
Content Signaling	Binary Floor Control Protocol (BFCP)	H.239	(Proprietary)
Conference Modes	Peer-to-peer, bridge (Advanced Video Coding (AVC), Scalable Video Coding (SVC))	Peer-to-peer, bridge (AVC)	Mesh, bridge (AVC)

WebRTC versus SIP Plug-in

At this time, WebRTC is a young and still-evolving technology. It offers end-users the advantage of joining a conference with their browsers without first having to install a plug-in, and it offers administrators the option of hosting mesh conferences that do not require MCU resources, thus improving the scalability of their infrastructure. But Polycom's browser plug-in still provides a better end-user experience in several respects, including:

- Support for HTTPS tunneling for better firewall traversal.
- Support for SVC (which provides a better user experience and puts less load on the infrastructure than AVC).
- Better error concealment and recovery.
- Better audio quality and echo cancellation.

For this reason, Polycom general philosophy is that if the user has already installed the SIP plug-in, it must be used to provide that better experience, particularly when mesh is not a concern.

RealPresence Web Suite Pro determines whether a client uses WebRTC or the plug-in based on the following criteria:

- The conference template used for the conference.
- Whether the client already has the plug-in.

- Whether its **Prefer SIP over WebRTC if plug-in is installed** setting is enabled (see [Enable WebRTC Support in the RealPresence Web Suite Pro System](#)).

The following table describes the behavior in the various scenarios:

WebRTC versus SIP plug-in selection criteria

Conference Template	Plug-in Absent	Plug-in Present
No WebRTC	Install plug-in	Use plug-in
WebRTC with MCUs only	Use WebRTC	Use plug-in
WebRTC with mesh only	Use WebRTC	Use WebRTC
WebRTC with MCUs or mesh	Use WebRTC	Depends on Prefer SIP over WebRTC if plug-in is installed setting

Thus the plug-in, if present, is always used for conferences using a *WebRTC with MCUs only* template. But you have the option of using a *WebRTC with MCUs or mesh* template, which lets you choose to prefer either the SIP plug-in, if present, for the best user experience or WebRTC for maximum infrastructure efficiency.

WebRTC Conference Modes

Polycom supports two WebRTC conference modes: mesh and bridge. A conference that begins in mesh mode can transition to bridge mode, as needed, given the proper configuration.

Mesh Conference Mode

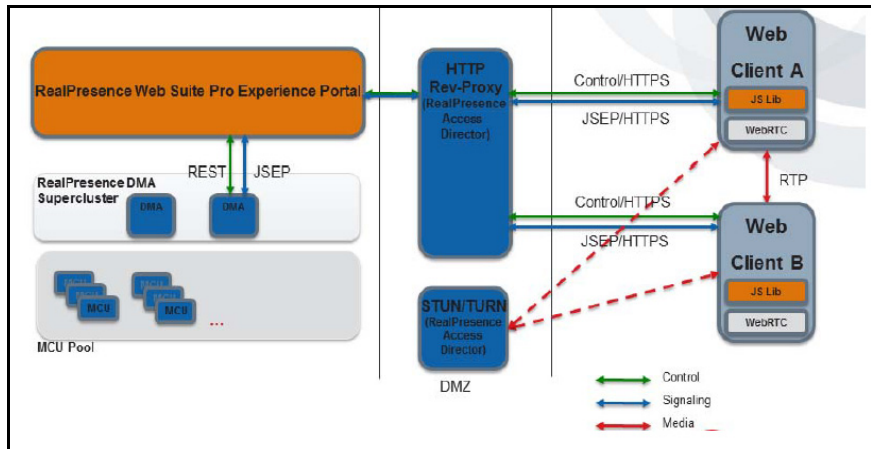
Mesh conference mode enables each web application (browser) to send media directly to the others in conference, rather than using an MCU (bridge). This means minimum server side resources are required to support the conference. An essential benefit of mesh meetings is the ability to run and manage a large number of mesh conferences simultaneously, which makes it a scalable video conferencing solution.

But mesh conferencing has the following limitations:

- Conference participants can only connect to a mesh meeting in a WebRTC-enabled browser.
- Because each participant receives media streams from all the others, bandwidth use grows quickly. *Mesh conferences are currently limited to three participants.*

The following diagram shows two WebRTC endpoints in a mesh conference.

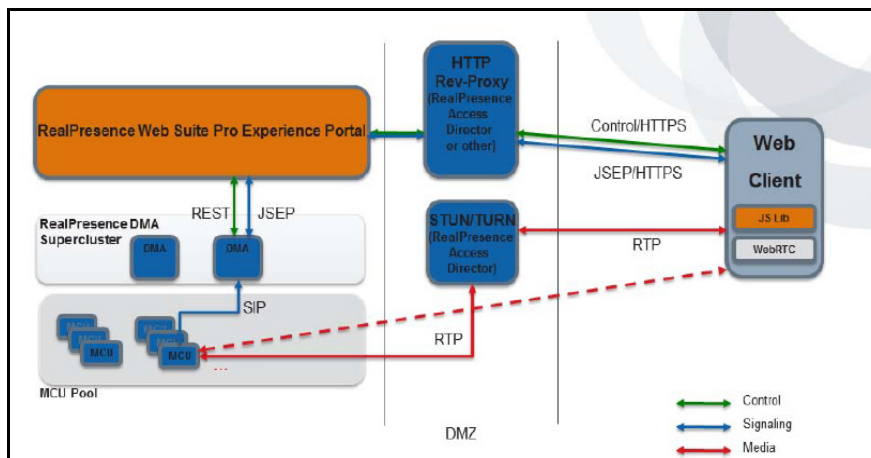
RealPresence Web Suite Pro: WebRTC Mesh Calls



Bridge Conference Mode

Bridge conferences are hosted on a WebRTC-enabled MCU. This enables WebRTC browser users to connect to any conference with participants of any type. It also enables a video conference to contain many more endpoints. The main drawback to bridge conference mode is the MCU resources required. The following diagram shows a WebRTC call to a WebRTC-enabled MCU.

RealPresence Web Suite Pro: WebRTC Call to MCU



Polycom WebRTC Deployment Assumptions and Scenarios

Although alternatives are mentioned when appropriate, the implementation described in this guide generally assumes and recommends the following about the environment and nature of the WebRTC solution deployment:

- The RealPresence Access Director system is used as the Session Traversal Utilities for NAT (STUN)/Traversal Using Relays around NAT (TURN) server, and it has the following characteristics:
 - It is deployed in the Demilitarized Zone (DMZ).
 - Its STUN/TURN service is homed on a single publicly reachable interface.

- That interface is typically an internal/private IP address that is mapped to an external/public address on the firewall using a static NAT mapping.
- The NAT must be set to a special mode that preserves the source IP address of packets sent to the RealPresence Access Director system external address.
- WebRTC ICE clients are given the public address of the RealPresence Access Director system STUN/TURN server.
- Firewall rules block inbound UDP traffic and may also disallow outbound UDP traffic except through the RealPresence Access Director system.
 - If outbound UDP is allowed from internal IP addresses to any external address over a wide range of ports, then media streams between internal and external devices typically use server reflexive candidates determined using STUN. This can reduce the load on the TURN server (the RealPresence Access Director system), but limits your organizational ability to control and monitor internal-to-external media flows.

Exception: If both the local firewall and remote firewall are symmetric NATs, which are not STUN-compatible, the clients must use a TURN relay candidate.

 - If outbound UDP traffic is blocked, then internal UDP connections are allowed only to the RealPresence Access Director system public TURN server IP address on UDP port 3478. In this case, media streams between internal and external devices always use a TURN relay candidate allocated by the internal client (mesh calls) or the MCU (bridge calls).
 - In either case, external UDP connections are allowed only to the RealPresence Access Director system public IP address on port 3478 or a port in the TURN relay range defined in the RealPresence Access Director system.

Media streams for external-to-external mesh calls use host candidates, server reflexive candidates, or relay candidates depending on the NAT/firewall situation of each endpoint.
- To protect against a malicious intrusion or DOS attempt using the TURN server as an attack vector/proxy, firewall rules must block inbound access from the RealPresence Access Director system TURN relay range into the organizational network.

Polycom WebRTC Solution Components

The sections that follow outline the required and optional parts of Polycom's WebRTC solution and describe the role of each required Polycom RealPresence product.

Required Solution Components

The following table lists the RealPresence products that are required in order to implement Polycom's WebRTC solution. Note that the RealPresence Web Suite system must have the Pro license. No special license is required for the other components.

Required WebRTC Solution Components

Polycom Product	Minimum Version	Function
RealPresence Web Suite with the Pro license	2.0	Supports WebRTC videoconferencing clients and enables audio and video browser-based clients that do not support WebRTC. Provides Enhanced Content Sharing services to WebRTC and other web browser clients. Provides clients with the TURN credentials they need to authenticate themselves to the TURN server (RealPresence® Access Director™).
RealPresence® DMA®	6.3	Supports signaling and management for WebRTC mesh and bridge (transcoded) calls. When bridge resources are needed, places calls on WebRTC-enabled RealPresence® Collaboration Server, Virtual Edition, MCUs.
RealPresence Collaboration Server, Virtual Edition	8.6	Supports WebRTC codecs (VP8 and OPUS) and media handling (ICE/STUN/TURN NAT/firewall traversal, SRTP-DTLS encryption, and Multiplexed RTP media streams), enabling WebRTC clients to join an MCU-hosted call.
RealPresence Access Director	4.2	Supports STUN and TURN server functions that enable NAT and firewall traversal for WebRTC clients.

Optional Solution Components

The following optional Polycom components may be used with Polycom's WebRTC solution.

- RealPresence Platform Director (2.0 or later) for licensing and monitoring component instances.
- RealPresence Media Suite (formerly RealPresence Capture Server) for recording and streaming meetings.
- RealPresence Resource Manager software for managing non-web-based endpoints, monitoring conferences, and other administrative functions.
- Polycom hard and soft endpoints, including:
 - Group Series
 - HDX
 - RealPresence Mobile
 - RealPresence Desktop

Supported Operating Systems and Web Browsers

For browser support and capability information, see the *RealPresence Web Suite Release Notes*. Note that due to issues with Firefox support for WebRTC and lack of feature parity, RealPresence Web Suite Pro does not currently support the use of Firefox with WebRTC. Firefox browser users can still be supported using the RealPresence Web Suite plug-in. See [Enable WebRTC Support in the RealPresence Web Suite Pro System](#).

RealPresence Web Suite Pro

RealPresence Web Suite Pro supports the following WebRTC functionality:

- WebRTC-enabled browser-based clients joining Polycom video conferences.
- Authentication using Enterprise Directory, with support for Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) Single Sign-On (SSO).
- Mesh and bridge-based conference modes.
- Conference roster for browser-based clients.
- Call control and chairperson features for browser-based clients.
- Enhanced content sharing, where supported by the browser and client platform and enabled in the RealPresence Platform infrastructure.
- Administrative configuration of WebRTC client support.

RealPresence Web Suite Pro User Features

The following WebRTC user features are supported in RealPresence Web Suite Pro:

- The ability to join conferences using a WebRTC-capable browser, if the RealPresence Platform infrastructure supports it and the administrator has enabled the use of WebRTC features on the server side.
- The ability to record conferences, if the RealPresence Platform infrastructure supports it.
- Enhanced content sharing using HTML5-compatible media.
- Consistent user interface and functionality for WebRTC and plug-in-based browser clients.
- Roster and chat functionality for managing and interacting with the other participants in the conference (chat is available only for browser-based clients, but the roster includes and can be used to control all endpoints in the conference).
- Plug-in availability for non-WebRTC-capable browsers and optionally for WebRTC-capable browsers.
- Automatic transition from mesh conferences to bridge (MCU-hosted) conferences.
- Content sharing capabilities for WebRTC endpoints.

RealPresence Web Suite Pro Server Features

The following WebRTC-related server features are supported in RealPresence Web Suite Pro:

- Support for the RealPresence Web Suite Pro WebRTC application and plug-in application.
- Enabling and disabling WebRTC calls.
- Relaying signaling messages between WebRTC clients and the RealPresence DMA system.
- Obtaining conference participant information from the RealPresence DMA system.
- Providing a roster of conference participants to browser clients.
- Providing an in-meeting chat service for browser clients.
- Enabling WebRTC clients to join passcode-protected conferences.
- Provisioning STUN and TURN information and authentication credentials for browser clients.
- Authenticating and authorizing WebRTC users either through local login credentials or Enterprise Directory.

RealPresence DMA System

In the RealPresence Platform WebRTC solution, the RealPresence DMA system provides the following:

- **Call and Conference Detail Records (CDRs)** Describes the history of each call and conference, including start time, end time, caller and callee information, and life-cycle events of the call or conference. You can use CDRs to either track usage patterns for Return On Investment (ROI) calculation or to generate billing records.
- **Active Call List** Provides a list of ongoing calls that is updated in real time for monitoring.
- **Call and Conference History** Provides a searchable list of historical calls and conferences, including detailed diagnostic data for troubleshooting.
- **Call and Conference Control APIs** Provides APIs for call and conference monitoring and control.
- **Network Usage Report** Provides historical usage data of network topology for capacity planning.
- **Site and Site Link Statistics** Provides real-time usage data of network topology for troubleshooting.

The RealPresence DMA system supports signaling and call control, enabling the following WebRTC features:

- **Mesh Conferences** Conferencing between browser clients where media is sent directly between clients, with no intermediate MCU.
- **WebRTC Connection to MCU-Based Conferences** Conferencing between browser clients and other endpoints, where media is relayed through a RealPresence Collaboration Server, Virtual Edition, MCU. Compared to mesh conferences, this reduces the number of media streams going to each endpoint, which reduces the CPU load on the clients and the total amount of network bandwidth consumed. Conferencing between browser clients and legacy standards-based endpoints using RealPresence Collaboration Server, Virtual Edition, as a media gateway allows web applications access to existing solutions.
- **Promotion of Mesh Conferences to MCU-Based Conferences** When the number of participants in a mesh conference would exceed the limit, a non-WebRTC endpoint wants to join the conference, or the chairperson elects to record the conference, the RealPresence DMA system automatically transitions the conference to an MCU-based conference, orchestrating the existing mesh attendees to redirect their media flows to the bridge.

RealPresence Collaboration Server, Virtual Edition

In the RealPresence Platform WebRTC solution, RealPresence Collaboration Server, Virtual Edition, provides the following:

- Support for the WebRTC VP8 (video) and Opus (audio) codecs
- Media transcoding between WebRTC codecs and other video and audio codecs (such as H.264 and SIREN)
- Datagram Transport Layer Security (DTLS)/Secure Real-time Transport Protocol (SRTP) support
- Interactive Connectivity Establishment (ICE) support
- RTP Bundling support

RealPresence Access Director

In the RealPresence Platform WebRTC solution, the RealPresence Access Director system provides video conferencing management for remote, guest, federated, and unfederated users with secure firewall traversal for the connections required.

To support WebRTC-based video conferencing, the RealPresence Access Director system supports both the STUN and TURN protocols. When needed, the RealPresence Access Director system can act as a TURN server to enable firewall and NAT traversal of UDP media traffic between WebRTC clients.

TURN is necessary when a WebRTC client wants to communicate with a peer but cannot do so because both client and peer are behind their respective NATs. If STUN is not an option because one of the NATs is a symmetric NAT (a type of NAT not compatible with STUN), TURN must be used for media relay.

When you enable and configure the TURN server and at least one TURN user, internal and external WebRTC clients can request TURN media relay services.

Refer to the *RealPresence Access Director System Administrator Guide* (available at [Polycom Support](#)) for more information about the network traversal services offered.



Note: Deploying RealPresence Access Director in a demilitarized zone with the TURN service

If RealPresence Access Director is deployed in a DMZ, you need to configure two externally-facing IP addresses for it: a private IP address to bind to the TURN service and a public IP address that maps the RealPresence Access Director TURN IP to the external firewall.

Implementing the WebRTC Solution

The RealPresence Platform WebRTC solution enables WebRTC-capable clients (such as Google Chrome browsers) to interoperate with SIP and H.323 clients and endpoints. This section provides high-level descriptions of how to enable and configure WebRTC across the RealPresence Platform products in order to implement support for it. It assumes the following:

- You have a properly configured and functioning RealPresence Platform environment that includes the components required to implement the WebRTC solution (see [Required Solution Components](#) in this guide and Getting Started Guide, Administrator Guide, and/or online help of each required component).
- RealPresence Web Suite Pro is working properly for SIP calls.
- The Enhanced Content feature in RealPresence Web Suite Pro has been enabled.



Note: WebRTC clients do not support video-based (H.264) content sharing

RealPresence Web Suite clients using WebRTC are unable to share content unless Enhanced Content is enabled. For this reason, Enhanced Content must always be enabled when WebRTC is in use.

We recommend following the order presented here to enable WebRTC for the environment. Refer to the documentation for each product (online help or *Administrator Guide*) for additional information and detailed procedures for each task.

Enable WebRTC Support in the RealPresence Access Director System

To support WebRTC, the RealPresence Access Director system must be configured to provide STUN/TURN and reverse proxy services. For detailed information about performing the tasks outlined below, refer to “TURN Services” in the Polycom RealPresence Access Director System Administrator Guide (available at [Polycom Support](#)) or the online help for the RealPresence Access Director **TURN Settings** page.



Note: The RealPresence Access Director TURN server provides both STUN and TURN services

STUN is a subset of TURN, so there is no need for separate STUN server configuration. TURN server configuration provides for both services.

To enable WebRTC in the RealPresence Access Director system:

- 1 In **Configuration > TURN Settings**, enable the TURN server and select the IP address of the network interface for external media relay as the **Listening IP**.
If you have separate internal and external media relay interfaces, you can enable TURN services on the internal interface and direct internal clients to it (by using split-horizon DNS to resolve the same Fully Qualified Domain Name (FQDN) differently for clients inside and outside the organization). Other options are possible. See “Configure TURN Settings” in the *RealPresence Access Director System Administrator Guide* for more information and consult your organizational IT staff if necessary.
- 2 If the system is in the DMZ, map the external media IP address (private) to the public address on the firewall and specify that as the **External IP Address of NAT**.
- 3 Specify the **TURN port (UDP)** and **Relay port range (UDP)**. We recommend leaving the default port (3478) and port range (49152–65535).
- 4 Specify the **Default authentication realm** (typically, your DNS, Windows, or Enterprise Directory domain). Polycom’s WebRTC clients always use the default realm.
- 5 Add a TURN user. Be sure to set this user **Realm** to the same value you specified as **Default authentication realm**.
Later, you specify this TURN user in the RealPresence Collaboration Server and RealPresence Web Suite Pro systems when enabling WebRTC in them. WebRTC clients must provide valid TURN user credentials in their TURN allocation requests (this is transparent to the person using the client); the RealPresence Web Suite Pro system provides them with these credentials.
Polycom recommends creating one TURN user to be used by all clients or one for browser TURN clients and another for MCU clients.
- 6 In **Configuration > Access Proxy Settings**, add an access proxy for TCP/HTTPS, specifying the RealPresence Access Director system external private IP address and port 443. Turn off both internal and external (client) certificate checking unless you are certain you need the additional security and understand what you are doing.
- 7 Add a next hop record of **Host header** type. For **Host value**, specify the FQDN used to access the RealPresence Web Suite Experience Portal (this FQDN must point to the RealPresence Access Director system external private IP address).
- 8 Set the **Address** of the next hop record to the IP address of the RealPresence Web Suite Experience Portal and **Port** to 443.

You will need to know the settings made on the RealPresence Access Director system in order to configure the RealPresence Collaboration Server, Virtual Edition, and the RealPresence Web Suite Pro system.

Enable WebRTC Support in the RealPresence Collaboration Server System

The RealPresence Collaboration Server, Virtual Edition, must be configured to support WebRTC media (VP8 video codec and Opus audio codec) and ICE STUN/TURN. No special license is needed. Only RealPresence Collaboration Server, Virtual Edition, MCUs (version 8.6 and later) support WebRTC. For detailed information about performing the tasks outlined below, refer to the *RealPresence Collaboration Server, Virtual Edition, Administrator Guide*.

To enable WebRTC in the RealPresence Collaboration Server, Virtual Edition:

- 1 On the **IP Network Services** page, verify that an IP service that is configured as a generic service already exists. If not, create one.



Note: The first IP service must be a generic service

An IP service must exist before adding a WebRTC service, and the existing service must be a generic service.

- 2 Add a new IP service with **IP Network Type** set to SIP or H.323 & SIP. Select the **Signaling Host IP Address** and **Media Card 1 IP Address** for this service.
- 3 On the **SIP Servers** tab of the dialog box, set **SIP Server Type** to WebRTC and leave the inbound and outbound SIP server fields blank.
- 4 On the **SIP Advanced** tab, configure the ICE environment for the WebRTC service, specifying the appropriate values from the RealPresence Access Director system configuration:
 - Set **STUN Server IP** to the IP specified as **External Address of NAT** in the RealPresence Access Director system (or the corresponding FQDN) and **STUN Server Port** to the TURN port in the RealPresence Access Director system (default 3478).
 - Set **TURN Server IP** and **TURN Server Port** to the **Listening IP** (or the corresponding FQDN) and TURN port specified in the RealPresence Access Director system.
 - Set the TURN server credentials to those of the TURN user you created in the RealPresence Access Director system.

The RealPresence Collaboration Server, Virtual Edition, must be rebooted in order for the changes made to take effect.

Enable WebRTC Support in the RealPresence DMA System

WebRTC signaling is on by default in the RealPresence DMA system. No special license is needed. Configuring the RealPresence DMA system to support WebRTC requires setting up at least one conference template configured for WebRTC (see step 5 below). If you intend to support WebRTC only for mesh conferences, no other configuration is necessary.



Note: To support guest callers, a dial rule for unauthorized calls is required

When a WebRTC caller connects to the RealPresence Web Suite Experience Portal as a guest (that is, the caller selects **Join as guest** on the login page), the RealPresence DMA system applies the dial rules for unauthorized calls (in **Admin > Call Server > Dial Rules**). There must be a dial rule for unauthorized calls with the action **Resolve to conference room ID** or the call fails. This rule is needed even if device authorization is not enabled. For information about setting up a dial plan for unauthorized calls, see the RealPresence DMA system online help for the Dial Rules page.

If you intend to support WebRTC for MCU-hosted conferences, you also need to configure MCUs into the appropriate pools and pool orders. What is appropriate depends on the MCUs you have and how they are configured.

Only RealPresence Collaboration Server, Virtual Edition, MCUs (version 8.6 and later) support WebRTC. In an environment with some MCUs that support WebRTC and others that do not, we recommend that you do the following:

- Put the MCUs configured for WebRTC into their own MCU pool and pool order, as described in the procedure below.
- Create a corresponding pools and pool order for non-WebRTC-supporting MCUs.
- Use separate conference templates for WebRTC-supporting conference rooms and non-WebRTC-supporting conference rooms.

These separations of WebRTC and non-WebRTC resources will help prevent under-utilization or over-utilization of some resources.

For detailed information about performing the tasks outlined below, refer to the RealPresence DMA system corresponding context-sensitive online help topics.



Note: MCU pool configuration not needed to support mesh only conferencing

If you intend to support only WebRTC mesh conferences, you can skip steps 2 through 4 in the procedure below.

To enable WebRTC in the RealPresence DMA system:

- 1 On the **Admin > Local Cluster > Signaling** page, verify that WebRTC signaling is enabled.
- 2 On the **Network > MCU > MCUs** page, determine which MCUs support WebRTC. Confirm that they have been configured properly to support WebRTC (see [Enable WebRTC Support in the RealPresence Collaboration Server System](#)).
- 3 Create an MCU pool or pools containing only MCUs that support WebRTC.
- 4 Create an MCU pool order containing the WebRTC-supporting MCU pools. Name it so that its purpose is clear when the list of pool orders is viewed in the RealPresence DMA Conference Rooms dialog or the RealPresence Web Suite Pro system.

You can also add pools containing MCUs that do not support WebRTC, but if an MCU that does not support WebRTC is selected for a conference, clients are unable to join using WebRTC. In any case, the first pool in the pool order must contain MCUs that support WebRTC.

- 5 On the **Admin > Conference Manager > Conference Templates** page, create one or more conference templates configured to support WebRTC in the desired manner.

A conference template can support WebRTC in one of the following ways:

- **WebRTC with mesh only** Supports only mesh conferences (limited to three WebRTC participants, and many template settings are disabled). Other types of endpoints will not be able to join VMRs created with a mesh only conference template.
- **WebRTC with MCUs only** Supports only MCU-hosted (bridge) conferences.
- **WebRTC with MCUs or mesh** Supports both mesh and MCU-hosted conferences. This setting enables a mesh conference to be moved to an MCU if a fourth WebRTC caller joins, if a non-WebRTC caller joins, or if certain conference features are needed, such as conference recording.

Be aware that a conference template that includes mesh conference support cannot be based on a conference profile, and certain template settings are disabled. Study the online help for Conference Templates carefully to understand the capabilities and limitations associated with WebRTC support.



Note: Mesh limit must remain 3 for compatibility with RealPresence Web Suite Pro

The latest version of the RealPresence DMA system includes the ability to change the maximum number of participants in a mesh call as an unsupported experimental feature. For compatibility with RealPresence Web Suite Pro, the conference template setting **Mesh limit** must remain at the default setting of 3.

- 6 On the **Admin > Call Server > Dial Rules** page, verify that there is a dial rule for unauthorized calls with the action **Resolve to conference room ID**. If not, add one.

Enable WebRTC Support in the RealPresence Web Suite Pro System

In order to support WebRTC, the RealPresence Web Suite Pro system must be connected directly or indirectly to a RealPresence DMA system that supports WebRTC. In addition, WebRTC must be enabled and configured in the administrator interface of the RealPresence Web Suite Experience Portal.



Note: Enable WebRTC in the RealPresence Web Suite Experience Portal last

Before enabling the RealPresence Web Suite Experience Portal for WebRTC support, make sure that:

- The RealPresence DMA system and the rest of your RealPresence Platform infrastructure have been provisioned appropriately to support WebRTC, as described in the preceding sections.
- Basic configuration of the RealPresence Web Suite portals is complete, including Enhanced Content.

To enable WebRTC in the RealPresence Web Suite Pro system:

- 1 In the RealPresence Web Suite Services Portal, navigate to **Settings > DMA Config** and add the RealPresence DMA system and its access points if you have not already done so. After the portal successfully connects to it, edit the system you added and select the appropriate MCU pool order and conference template for WebRTC. See [Add a RealPresence DMA System and Access Points](#).
- 2 In the administration interface of the RealPresence Web Suite Experience Portal, navigate to **Conference > Conference**. Under **Agents**, expand **DMA** and configure an agent to communicate with the RealPresence DMA system added in the RealPresence Web Suite Services Portal if you have not already done so. See [Configure the RealPresence DMA Agent](#).
- 3 Still in **Conference > Conference**, under **Agents**, expand **WebRTC** and **Settings** to configure WebRTC support, as described in the following table.

Field Name	Value/Description
DMA Target URL	Populated based on the RealPresence Web Suite Services Portal DMA agent configuration and cannot be edited.
Enabled	Select to enable WebRTC support.
Prefer SIP over WebRTC if plug-in is installed	If selected, RealPresence Web Suite Pro clients that have the RealPresence Web Suite audio-video plug-in installed always attempt to connect to a VMR using the SIP protocol, unless it is a mesh-only meeting. They use WebRTC only if the plug-in is not installed (and the other criteria for using WebRTC are met). If not selected (the default), WebRTC-capable clients use WebRTC to place a call to any VMR whose conference template supports WebRTC for mesh only or mesh and MCU meetings, even if the plug-in is installed. They still use the plug-in for calls to VMRs whose template supports WebRTC for MCU only or does not support WebRTC.
Enable WebRTC support in Firefox	If selected, RealPresence Web Suite Pro clients using the Firefox browser can use WebRTC. Due to limitations in Firefox support for WebRTC, we recommend selecting this option only for testing/evaluation purposes. If not selected (the default), Firefox browsers use the RealPresence Web Suite plug-in to place SIP calls.
Max Chrome Version	Allows you to specify the maximum major version number of the Chrome browser (for instance, 45 or 46) for which RealPresence Web Suite supports WebRTC. If the major version number of the caller is greater than this value, and the conference template for the meeting is set to WebRTC with MCUs only or WebRTC with MCUs or mesh, the caller is prompted to install and use the RealPresence Web Suite plug-in. This setting is only necessary if a Chrome update makes changes to the low-level behavior of the browser that are incompatible with the RealPresence Platform WebRTC solution. In that case, setting this value appropriately ensures that users of the incompatible Chrome version can still successfully join MCU-enabled meetings by using the plug-in. Note: • Users of incompatible Chrome versions will not be able to join mesh-only meetings. • Polycom strives to provide timely updates to address such compatibility issues, so if this setting is needed, it must only be needed temporarily. • The latest browser compatibility information is in RealPresence Web Suite Release Notes and applicable Polycom Tech Alerts.

Field Name	Value/Description
Use relay candidates only	Determines the ICE candidate selection policies used by WebRTC clients when sending their audio and video media in scenarios requiring NAT/firewall traversal. If selected, external clients ignore WebRTC server reflexive and host candidates and only consider relay candidates allocated using the TURN server (typically, the RealPresence Access Director TURN relay service). If not selected (the default), clients attempt to send media directly peer-to-peer where feasible, using server reflexive candidates gathered using the STUN or TURN protocols. Note: This flag is intended for temporary use to validate that your TURN set-up is functioning correctly. For production operation, it must generally be disabled.
Call Rate Settings	Specify the line rates used for WebRTC. The defaults are 512 Kbps for WebRTC mesh calls and 384 Kbps for WebRTC bridge calls. Typically, the line rate is set fairly high in the RealPresence DMA conference template for the benefit of non-WebRTC endpoints. But if a WebRTC client browser attempts to transmit data at such a high rate, audio and video quality are likely to suffer. These settings prevent that. Note: The 384 Kbps default for bridge calls is a conservative setting chosen to provide a more predictable experience for remote callers connecting over consumer-grade public networks (such as 3G cellular, marginal WiFi, or slow DSL). If the environments of your remote users can support a higher bit rate, you can increase this setting to provide better video quality.
STUN Settings	Specify one or more STUN servers by IP address or FQDN. The default port number (3478) is used unless you specify a different one. Note: If you specify one or more TURN servers in the TURN Settings field below, you generally do not have to enter the same address in the STUN Settings field. TURN is a functional superset of STUN and generates both server reflexive and relay candidates from the specified server. The RealPresence Access Director TURN server provides both STUN and TURN services. WebRTC clients use the specified STUN servers to make STUN binding requests in order to generate server reflexive ICE candidates. The ICE algorithm determines which candidates to use for the actual media exchange.
TURN Settings	Specify one or more TURN servers by IP address or FQDN. The default port number (3478) is used unless you specify a different one. Provide the TURN user credentials for each TURN server (the credentials you defined on your RealPresence Access Director or other TURN server). The RealPresence Web Suite Experience Portal provides these credentials to WebRTC clients so that they can connect to the TURN servers. WebRTC clients use the specified TURN servers to make TURN allocation requests in order to generate server reflexive and relay ICE candidates. The ICE algorithm determines which candidates to use for the actual media exchange.

Appendix 2: Set Up Enterprise Directory for Single Sign-On

Before setting up the Single Sign-on (SSO) configuration in the RealPresence Web Suite Services Portal, you must set up your Enterprise Directory server to support SSO. The sections that follow describe how to do so.



Caution: Install CA-signed certificates before continuing

Before enabling SSO, ensure that the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal have certificates signed by a commercial Certificate Authority (CA), not self-signed certificates. See [Manage Certificates and Certificate Signing Requests](#).

Polycom strongly recommends installing certificates signed by a commercial CA in all components of the RealPresence® Platform solution.

Complete the following tasks in Enterprise Directory to support SSO:

- 1 [Create a RealPresence Web Suite Services Portal User Account in Enterprise Directory](#)
- 2 [Set a Service Principal Name for the RealPresence Web Suite Services Portal User Account in Enterprise Directory](#)
- 3 [Generate a Keytab File for the RealPresence Web Suite Services Portal User](#)

Create a RealPresence Web Suite Services Portal User Account in Enterprise Directory

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

To create a RealPresence Web Suite Services Portal user in Enterprise Directory:

- 1 Log in to the appropriate Enterprise Directory domain with administrator credentials.
- 2 Navigate to **START > Control Panel > Administrative Tools > Active Directory Users and Computers**.
- 3 Create a user account (not a machine account) for the RealPresence Web Suite Services Portal service.

Polycom recommends that the user account name be the same as the Domain Name System (DNS) host name of the RealPresence Web Suite Services Portal server.

- 4 Set a password for the RealPresence Web Suite Services Portal user account. Make note of the password; you will need it later.

Set a Service Principal Name for the RealPresence Web Suite Services Portal User Account in Enterprise Directory

After creating the Enterprise Directory user account for the RealPresence Web Suite 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 Web Suite Services Portal user account.

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

- 1 In the Enterprise Directory domain server, navigate to **Start > Control Panel > Administrative Tools > ADSI Edit**.
- 2 Find the RealPresence Web Suite Services Portal user you created.
- 3 Open the user properties, and update **servicePrincipalName** using the following format:

`HTTP/<wsp_server_host_name>.<AD_domain_name>@<AD_DOMAIN_NAME>`

For example, if the RealPresence Web Suite Services Portal (WSP) host name is `wsp-sso` and the Enterprise Directory domain is `cloudax.is`, the **servicePrincipalName** value would be:

`HTTP/wsp-sso.cloudax.is@CLOUDAX.IS`

Polycom recommends that the RealPresence Web Suite Services Portal server and Enterprise Directory server be in the same Active Directory domain. But if your network setup requires that they be in different domains, the **servicePrincipalName** can be specified as follows:

`HTTP/<wsp_server_fqdn>@<AD_DOMAIN_NAME>`

For example, if the RealPresence Web Suite Services Portal (WSP) host name is `wsp-sso`, its domain is `cloudax.is`, and the AD domain is `example.com`, the **servicePrincipalName** value would be:

`HTTP/wsp-sso.cloudax.is@EXAMPLE.COM`

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

- 4 Save the updated user settings.

Generate a Keytab File for the RealPresence Web Suite 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 Enterprise Directory server for the RealPresence Web Suite Services Portal service and upload it to the RealPresence Web Suite Services Portal when configuring SSO.

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 sensitive 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 Web Suite Services Portal user:

- 1 Log in to the Enterprise 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, if the WSP host name is wsp-sso, the user password is Polycom123, and the Enterprise Directory domain is cloudax.is, the command would be:

```
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 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 3: Create an App to Access Google+ Social Media Contacts

You can set up the RealPresence Web Suite environment so that users can invite contacts from their personal Google+™ accounts to meetings. But first you must create a custom app in Google to connect user social networking contacts with the RealPresence Web Suite user environment.



Note: Facebook® and LinkedIn® application creation is no longer supported

Facebook and LinkedIn contacts are no longer supported. To add Facebook or LinkedIn contacts to a RealPresence Web Suite meeting, users can send them an invitation by email or send the meeting details in a message on Facebook or LinkedIn.

Before you begin, set up a neutral Google account with credentials that can be shared among different members in your team. To avoid dependencies on a single person, do not use any other personal Google account to create the application. If the person currently responsible for the application leaves your organization, the common account credentials can be passed on to the team.

After you create the Google application, you must enable it in the RealPresence Web Suite Services Portal (see [Configure Social Network Access](#)).

Because the [Google Developers Console](#) is prone to change from time to time, the instructions here are general. For specific information about the steps, refer to the [Google Developers Console Help](#) website.



Note: The Google application is only for the RealPresence Web Suite Services Portal for which you created it

The Google application you create is specific to the Fully Qualified Domain Name (FQDN) of the RealPresence Web Suite Services Portal; it cannot be used for a different RealPresence Web Suite Services Portal or if you change the FQDN. But an IP address change does not require a new app as long as the same FQDN resolves to the new IP address.

Always maintain one-to-one mapping between the RealPresence Web Suite Services Portal server and the Google app.

To create a Google+ application:

- 1 Log in to the shared Google account.
- 2 Open the [Google Developers Console](#) page and create a new project.
- 3 Add the Google+ API to the project.
- 4 Complete the OAuth consent screen and create an OAuth client ID.
 - For Application type, select Web application.
 - For Authorized JavaScript Origins, enter the RealPresence Web Suite Services Portal FQDN.
 - For Authorized Redirect URIs, enter:
`https://<ServicesPortalFQDN>/wsp/wspconnect/connect/google`

- 5** Make note of the client ID and client secret fields, which are needed to enable social network contacts in the RealPresence Web Suite Services Portal.

Appendix 4: Cookies Used

The RealPresence Web Suite Services Portal uses the following cookies:

- **WSP Application** Uses the userToken=0B8A4F41-AF5A-8809-6D34-F583AB7B5D06 and loginUser=admin cookies for requesting secure back-end API calls.
- **userRole=ROLE_SUPER_ADMIN, ROLE_ADMIN, ROLE_USER** Specifies the user account role, which determines the user capabilities. See [Account Roles](#).
- **i18next – en-US** i18Next library sets this cookie to handle internationalization for the RealPresence Web Suite Services Portal.

The RealPresence Web Suite Experience Portal uses the following cookies:

- **ManualLogin** This session cookie is a Boolean value used by the RealPresence Web Suite Experience Portal to determine if a login session was initiated by a user login or by an application integration or Single Sign-on (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 email 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 log back in again 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 5: Conference Template 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 factory conference template settings on RealPresence Web Suite operations. For information on setting up a RealPresence DMA system conference template, see the *Polycom RealPresence DMA 7000 System Operations Guide* (available at [Polycom Support](#)).

Conference Template Settings Impact

Feature	Sub Feature	Sub Feature Description	Web Client Behavior	
General settings	Profile settings	Use existing profile	Not applicable	
		RealPresence Collaboration Server (RMX) profile name	Works as documented	
Conference settings	Conference mode		Both Advanced Video Coding (AVC) and Scalable Video Coding (SVC) are supported. If AVC only is selected, the RealPresence Web Suite web client operates in AVC (transcoded media) mode. If SVC only or Mixed AVC and SVC is selected, the RealPresence Web Suite 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
		LPR		Works as documented

Conference Template Settings Impact

Feature	Sub Feature	Sub Feature Description	Web Client Behavior
Video quality	People video definition	Video quality	Works as documented
		Max resolution	Works as documented
		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		To support Enhanced Content Sharing, set this to false to prevent ECS clients from receiving a redundant content view in their people video channel.
	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	
Keyboard noise suppression		Works as documented	
Audio clarity		Works as documented	
Skins			Works as documented
Conference IVR	Override default service		Advanced—see the <i>Polycom RealPresence DMA 7000 System Operations Guide</i>
	Conference IVR service		May require use of Dual-tone Multi-frequency (DTMF) pad in menu
	Conference requires chairperson		Users wait in the lobby until the chairperson joins the conference.

Conference Template Settings Impact

Feature	Sub Feature	Sub Feature Description	Web Client Behavior
Recording	Record conference		Must be set to Immediately or Upon Request to enable recording
	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.

Appendix 6: Log Management

This section describes the RealPresence Web Suite Log Management for capturing both server-side logs and client-side logs.

This section includes the following topics:

- [Additional Required Information for Debugging Issues](#)
- [Server-side Logs](#)
- [RealPresence Platform Component Logs](#)
- [Client-side Logs](#)
- [Web Client Console Logs](#)

Additional Required Information for Debugging Issues

The following is additional information required to troubleshoot issues beyond the information contained in the log files:

- Lobby Code
- Meeting ID (VMR Number)
- Time of Incident
- User ID of the impacted user
- Email ID of the impacted user
- Processor

The following additional information is required to troubleshoot media-related issues:

- RAM
- OS version
- Video memory
- Camera type (internal/external)
- Graphics card type

Server-side Logs

The Server-side logs include logs collected and downloaded from RealPresence Web Suite Services Portal (Web Services Portal [WSP] Server) and RealPresence Web Suite Experience Portal (Meeting Experience Application [MEA] Server). The RealPresence Web Suite Client software automatically writes log data to the browser console.

You can configure the RealPresence Web Suite Services Portal and RealPresence Web Suite Experience Portal to collect the client console logs on the portal as a compressed archive.

- For instructions on setting server log levels and downloading the WSP server-side log files, see [Manage RealPresence Web Suite Services Portal Logging and Data Collection](#).
- For more information on setting server log levels and downloading MEA server-side log files, see [Manage RealPresence Web Suite Experience Portal Logging](#), and for MEA server-side logs (SSH), see [Collect log files](#).

RealPresence Platform Component Logs

When reporting media or signaling-related issues, Polycom recommends collecting logs from the following RealPresence Platform components:

- [Capture RealPresence DMA Logs](#)
- [Capture RealPresence Collaboration Server \(RMX\) Logs](#)
- [Capture RealPresence Access Director Logs](#)



Note: Include the time when the incident occurred

Polycom recommends to include the time when the incident occurred when providing log files.

Capture RealPresence DMA Logs

You can provide information from RealPresence DMA by capturing system log files.

To capture system logs from RealPresence DMA:

- 1 Launch the RealPresence DMA URL using `https://<ipaddress>:8443/dma700`.
- 2 Log in with admin credentials.
- 3 Navigate to **Maintenance > System Log Files**.
- 4 Download the active logs.



Note: You may be prompted to manually roll logs after downloading the active logs

You may be prompted to manually roll logs to start gathering fresh data.

After a certain amount of collection time, you may be asked to download the active logs and send them to Polycom Global Services.

Apart from the system logs, RealPresence DMA also supports collecting the call report for any specific user or Virtual Meeting Room (VMR).

To collect call reports for users and VMRs:

- 1 Navigate to **Admin > Reports > Call History**.
- 2 Select the call that the user wants to troubleshoot.

- 3 On the right-hand column, select **Show Call Details**.
- 4 On the pop-up window, select the different options to show relevant information about the call.
- 5 If the RealPresence DMA version is 6.3.1 or above, select **Signaling Diagram** and download the Call Flow Ladder diagram.



Note: You can control the log level by configuring the options

For the RealPresence DMA system logs, you can control the log level by using the options available under **Admin > Local Cluster > Logging Settings**.

Capture RealPresence Collaboration Server (RMX) Logs

You can provide information from RealPresence Collaboration Server (RMX) by capturing system log files.

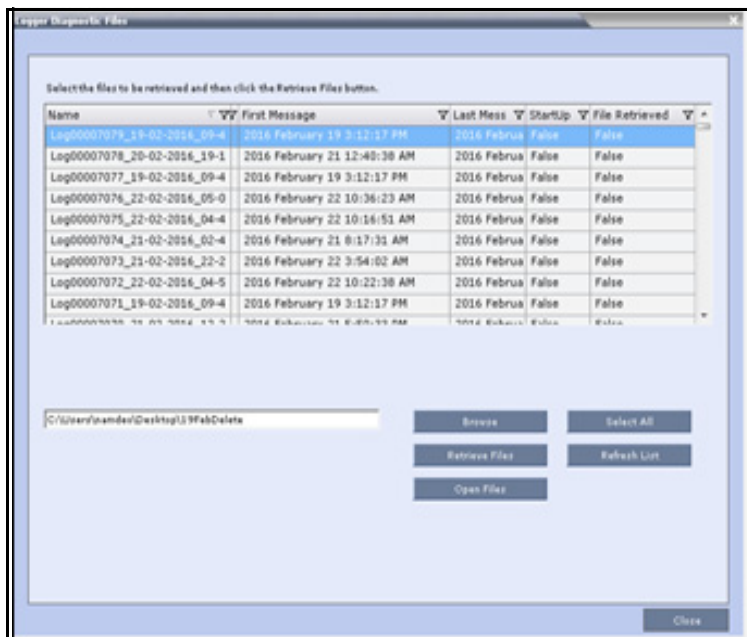


Note: Use Internet Explorer to access the RealPresence Collaboration Server (RMX) Admin UI

Internet Explorer is the only supported browser to use to access the RealPresence Collaboration Server (RMX) Admin UI..

To collect RealPresence Collaboration Server (RMX) logs:

- 1 Open the RealPresence Collaboration Server (RMX) EMA UI by using Internet Explorer, or use the RMX Manager to view the RealPresence Collaboration Server (RMX) admin UI.
- 2 Log in with admin credentials.
- 3 Navigate to **Tool > Administration > Logger Diagnostic Files**.

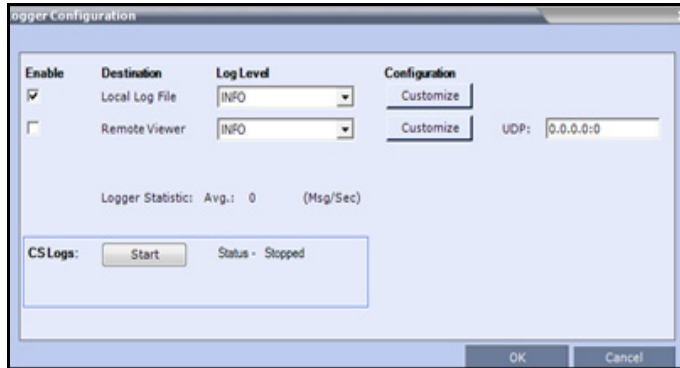


- 4 Select the files based on the time stamp when the issue is observed and click **Browse**.

- 5 Locate the folder and click **Retrieve Files**.

To capture the MCU logs:

- 1 Start the RealPresence Collaboration Server logs by navigating to **Administrator > Tools > Logger Configuration**.
- 2 Select the log level and start the RealPresence Collaboration Server logs on the pop-up window that appears.



- 3 Capture the TCPDUMP by navigating to **Administrator > Tools > Network Traffic capture**.
- 4 Collect the additional system logs by navigating to **Administrator > Tools > Information Collector**.
- 5 Select the date, time, and the system log types that are to be captured.
- 6 Click **Collect Information** to download a zip file to your specified location.

Capture RealPresence Access Director Logs

Before downloading the System Log file, enable the different types of packets that are to be captured by navigating to **Admin > Diagnostics > Traffic Capture**.

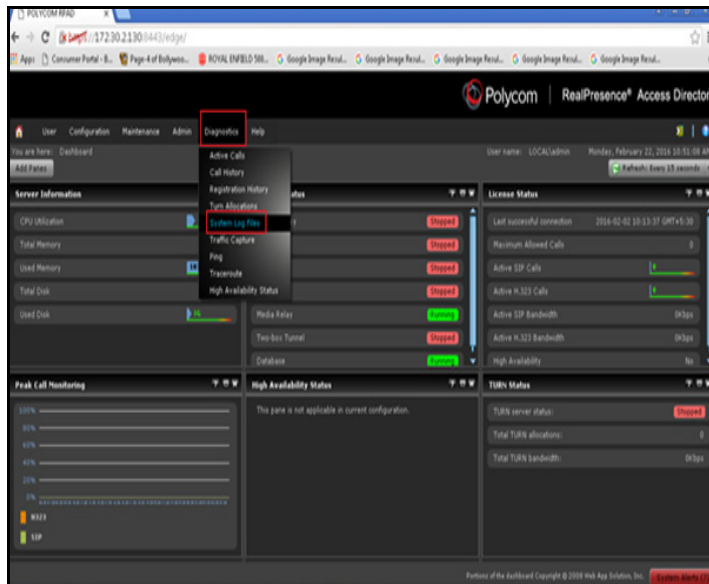


Note: Navigate to Call History page for more information about the call

You can also navigate to the **Call History** page to get more information about the call.

To capture the system logs from RealPresence Access Director:

- 1 Open the RealPresence Access Director Admin UI using <https://<ipaddress>:8443/edge/>.
- 2 Log in with admin credentials.
- 3 Navigate to **Diagnostics > System Log Files**.



4 Download and attach the log files.

Client-side Logs

The Client-side logs include logs collected on the client side (the user's PC or laptop), where the RealPresence Web Suite client is running.

You can collect client-side logs on the following systems:

- [Collect Primary Client Logs on Windows](#)
- [Collect Primary Client Logs on Mac](#)
- [Collecting MEA Server and WSP Client Logs](#)

Collect Primary Client Logs on Windows

You can provide information from RealPresence Web Suite by capturing Windows system log files.

To collect primary client logs on Windows systems:

- 1 Use File Explorer to navigate to: %appdata%/../LocalLow/Polycom.
- 2 Create a temporary directory (for example, "Call1").
- 3 Select the *.log files specific to the time of the incident and copy them to the temporary directory.
- 4 Zip the temporary directory.
- 5 Delete the unzipped temporary directory.
- 6 Provide the zipped directory to your system administrator or to Polycom for troubleshooting.

Collect Primary Client Logs on Mac

You can provide information from RealPresence Web Suite by capturing Mac system log files.

To collect primary client logs on Mac systems:

- 1 Use the **Finder** menu option and navigate to **Go > Go to Folder**.
- 2 Enter **~/Library/Logs** for the folder name. This will switch the current Finder window to the directory that includes the log files.
- 3 Select the log files specific to the incident from the Polycom folder. Right-click or **Ctrl+click** the selected log files and select the **Compress** option. This creates a ZIP archive and retains the log files in the Polycom folder.
- 4 Provide the zipped directory to your system administrator or to Polycom for troubleshooting.

Collecting MEA Server and WSP Client Logs

You can also collect logs on the MEA Server and WSP client by using tcpdump or Wireshark. The collection of these logs help in identifying and isolating issues that might have resulted because of the network problems.

Collecting Logs for MEA Server

Polycom, by default, does not install and ship the TCPDUMP application with the Linux OS running on the MEA Server. User must install LIBCAP and TCPDUMP RPM packages on the MEA Server.

Collecting Logs for WSP Client

Wireshark is a third-party network packet capture and analyze tool. Wireshark is directly downloaded from internet and used on the PC or laptop running the WSP client.

Web Client Console Logs

You can enable enhanced logging using the following methods:

- [Enable Enhanced Log Level for Web Client Console Logs](#)
- [Collect Enhanced Logs in the RealPresence Web Suite Services Portal](#)
- [Enable Enhanced Logging on Google Chrome](#)

The web client console logs include browser console logs collected on any of the following:

- [Web Client Console Logs—Google Chrome](#)
- [Web Client Console Logs—Mozilla Firefox](#)
- [Web Client Console Logs—Internet Explorer](#)

The browser console logs are helpful for reporting the issues such as:

- Call disconnects
- Video layout issues such as black video cells in the main video window or thumbnails during SVC calls
- Other UI issues (overlapping or rendering issues associated with UI elements, for example)

Enable Enhanced Log Level for Web Client Console Logs

You can enable enhanced log level collection for web client console logs.

To enable enhanced log level for web client console logs:

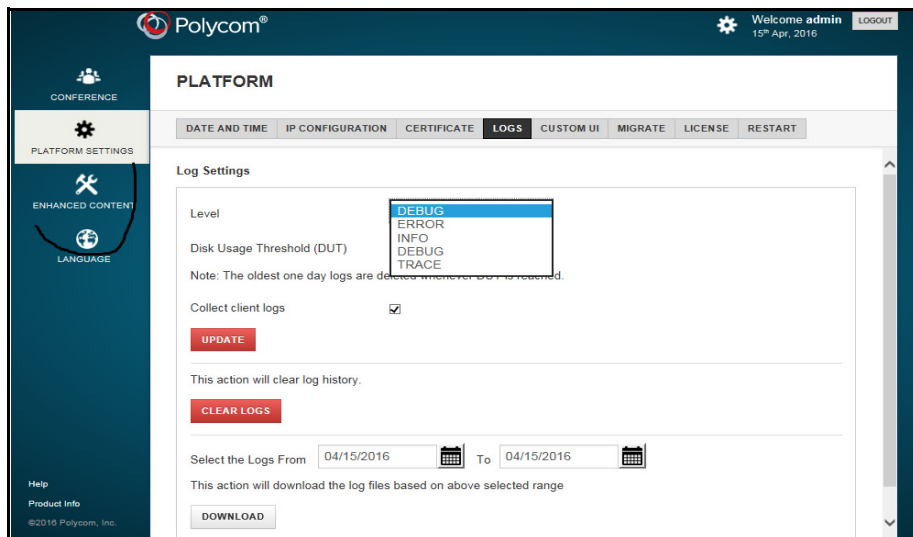
- 1 Launch a RealPresence Web Suite Experience Portal session using the URL (not by clicking the URL published by the RealPresence Web Suite Services Portal).
- 2 Enter the lobby code or Virtual Meeting Room (VMR) to join the meeting.
- 3 Press **F12** to open the JavaScript console, and type the following commands sequentially.
 - a `document.cookie = 'always_debug=true'`
 - b `document.cookie = 'always_trace=true'`
 - c `document.cookie = 'enable_remote_logging=true'`
- 4 End the meeting and restart the browser.

Collect Enhanced Logs in the RealPresence Web Suite Services Portal

Another option is to collect enhanced logs in directly from the RealPresence Web Suite Services Portal.

To collect enhanced logs in the RealPresence Web Suite Services Portal:

- 1 Log into the RealPresence Web Suite Services Portal with admin credentials.
- 2 Set the log level to **Debug** and check **Collect client logs**.



Note: Do not enable this option for long durations

Do not enable this option for long durations, because it impacts product performance as many device I/O operations will be performed periodically.

Enable Enhanced Logging on Google Chrome

The following is the URL for enabling Chrome debug logging:

<http://www.chromium.org/for-testers/enable-logging>

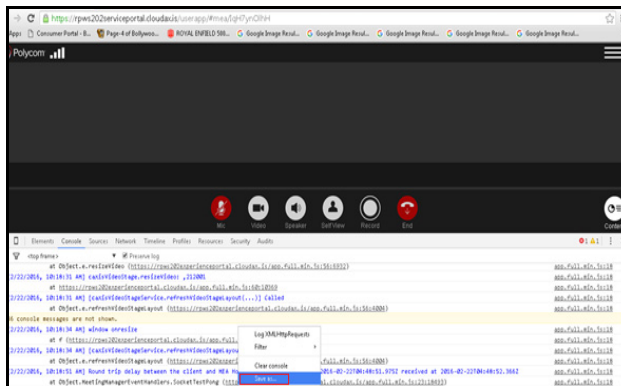
OS Type	Debug Logging Steps
Windows	Navigate to Google Chrome Shortcut properties and add this string at the end in Target: <pre>--enable-logging --v=1 --no-sandbox</pre> The Windows log file is saved in the following path: <pre>C:\Users\<username>\AppData\Local\Google\Chrome\User Data\chrome_debug.log</pre>
Mac	Launch Chrome from the Mac Terminal: <pre>/Applications/Google\ Chrome.app/Contents/MacOS/Google\ Chrome</pre> <pre>--enable-logging --v=1</pre> The Mac log file is saved in the following path: <pre>~/Library/Application\ Support/Google/Chrome/chrome_debug.log</pre>

Web Client Console Logs—Google Chrome

You can collect web client console logs directly from Google Chrome.

To collect the client console logs on Google Chrome:

- 1 Press **F12** on the web client call session window.
- 2 Navigate to **Console** tab.
- 3 Right-click the console window and select **Save As**.
- 4 Save the logs and attach with the other logs.

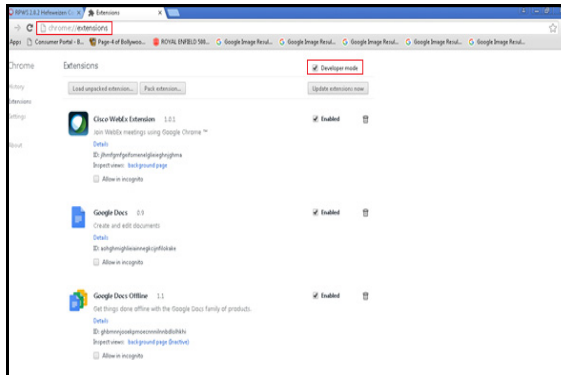


Additional Debugging for Chrome

You can perform additional debugging on Chrome.

To perform additional debugging on Chrome:

- 1 When the call is active, open another tab.
- 2 In the address bar type **chrome://extensions**.
- 3 On the extension window, select the **Developer Mode** check box.



- 4 Locate the Polycom RealPresence Web Suite extension. Then select **background.xml**.
- 5 On the window that appears, type **logger.enableLogging()** next to ">" symbol.
- 6 Right-click the console window and select **Save As**.
- 7 Save the logs and attach with the other logs.

Chrome Mini-Dumps

The following are the mini-dumps for Chrome:

OS Type	Mini-dump Path
Windows	Candidates: • C:\Users\{username}\AppData\Local\Google\CrashReports • C:\Users\{username}\AppData\Local\CrashDumps • C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Crash Reports
Mac	~/Library/Application Support/Google/Chrome/Crashpad/completed

Web Client Console Logs—Mozilla Firefox

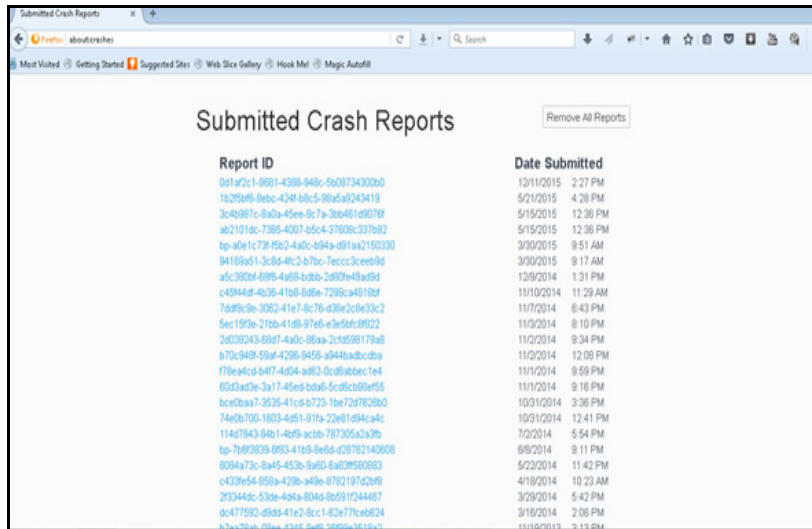
You can collect web client console logs directly from Mozilla Firefox.

To collect the web client console logs on Mozilla Firefox:

- 1 Press **F12** on the web client call session window.
- 2 Navigate to **Console** tab.
- 3 Click anywhere on the console window.
- 4 Press **Ctrl+A**, and ensure all the text in the console window is selected.
- 5 Press **Ctrl+C** to copy all the logs.
- 6 Open any text editor, for example: WordPad, Microsoft Word, or Notepad++.
- 7 Paste the text, save it, and attach with the other logs.

To collect crash data in Mozilla Firefox:

- 1 Open the Firefox browser in a separate tab or window.
- 2 Type **about:crashes** in the address bar.



Report ID	Date Submitted
0d1a2c1-9891-4389-948c-5d08734300d0	12/11/2015 2:27 PM
1b2f9f9b-8ebc-424f-8bc5-88a5a0434119	5/21/2015 4:28 PM
3c4b987c-8a0a-45ee-8c7a-3bb481d9070f	5/15/2015 12:36 PM
ab2101dc-7365-4007-a5c4-37808c337692	5/15/2015 12:36 PM
bp-a0e1c73f-45b2-4a0c-894a-d91aa2150330	3/30/2015 9:51 AM
94168a51-3c8d-46c2-b7bc-7eccc3ceebfd	3/30/2015 9:17 AM
a5c382bf-6985-4a08-b2bb-2a80fe8ba5d1	12/9/2014 1:31 PM
c4944af-4b36-41b8-836a-7290ca4818bf	11/10/2014 11:29 AM
7d9f9c9e-3082-41e7-8c76-d38a2c8e33c2	11/7/2014 6:43 PM
5ec15f3e-21bb-41b8-91e8-e3e8bfc89222	11/2/2014 8:10 PM
2a038243-68d7-4a0c-86aa-2c8f588179a8	11/2/2014 9:34 PM
b70c948f-58af-4296-9456-a944abcbda	11/2/2014 12:08 PM
f78e4cd4-b477-4d04-a982-0c0fabbec1e4	11/1/2014 9:59 PM
60d3ad3e-3a17-45e8-bda6-5cd8c88e9f55	11/1/2014 9:16 PM
bce0baa7-3c35-41c8-8723-1be72d7629d0	10/31/2014 3:38 PM
74e0b700-1803-4a51-91fa-22a81d94c44c	10/31/2014 12:41 PM
114d7843-84b1-4b09-accb-787305a2a39b	7/2/2014 5:54 PM
bp-7b8783b8-8953-41b8-8e8d-d28782140008	6/9/2014 9:11 PM
8084a73c-6a45-452b-8a00-6a039580893	5/22/2014 11:42 PM
c4339e54-850a-429b-a40e-8782197d2b0f	4/18/2014 10:23 AM
2f3344ac-53de-494a-8046-0b591f244467	3/29/2014 5:42 PM
dc477592-d9d8-41e3-8cc1-82e777ceeb24	3/18/2014 2:08 PM
b7ca780a-0ba6-4a0f-8a08-0a080a0a0a0a	11/10/2013 7:13 PM

- 3 Open the log files based on the time stamp.
- 4 Save the log file as a.pdf and attach with the logs.

Web Client Console Logs—Internet Explorer

You can collect web client console logs directly from Internet Explorer.

To collect the web client console logs in Internet Explorer:

- 1 Press **F12** on the web client call session window.
- 2 Navigate to **Console** tab.
- 3 Click anywhere on the console window.
- 4 Press **Ctrl+A**, and ensure all the text in the console window is selected.
- 5 Press **Ctrl+C** to copy all the logs.



Note: You can copy all logs

Right-clicking the console tab gives an option to copy all logs.

- 6 Open any text editor, for example: WordPad, Microsoft Word, or Notepad++.
- 7 Paste the text, save it, and attach with the other logs.