



ADMINISTRATOR GUIDE

Version 3.0 | March 2016 | 3725-66008-002A

Polycom[®] RealPresence[®] Platform Director[™]



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.

About This Guide	7
Audience, Purpose and Required Skills	7
Downloads	7
Reference Documentation	7
Conventions Used in this Guide	7
Terms Used in this Guide	8
Get Help	9
Polycom and Partner Resources	9
The Polycom Community	9
Documentation Feedback	9
Product Overview	10
Deployment Scenario in A vCenter Environment,	10
Managing and Configuring the RealPresence Platform Director Environment	12
vCenter Only: Managing Providers	12
Add a Provider	12
Edit a Provider	13
Delete a Provider	13
Managing Zones	13
Add a Zone	14
Edit a Zone	14
Delete a Zone	15
vCenter Only: Managing Resource Groups	15
Add a Resource Group to a Zone	15
Edit a Resource Group	16
View Resource Group Status	16
Delete a Resource Group	17
Managing Service Groups	17
Create a Service Group	18
View or Edit Service Group Details	18
Add a New Instance to a Service Group	18
Remove an Instance from a Service Group	19
vCenter Only: Managing Virtual Edition Images	19
Add a Component Virtual Edition Image	19
Edit Image Values	20
Delete an Image	21
Adding Instances	21
Create Instance (vCenter Only)	22
Add Existing Virtual (vCenter Only)	24

Add Existing by IP	26
Add Appliance with Legacy Licensing	27
View or Edit Instance Details	28
Delete an Instance	28
Managing RealPresence Platform Product Licenses	29
Online and Offline Mode	30
Allocate Licenses for Polycom RealPresence Platform system Components	30
Update the Licenses of Polycom RealPresence Platform system Components	31
View RealPresence One License Usage Report	32
Monitoring the RealPresence Platform Director Environment	35
SNMP Description	35
SNMP Framework	35
Supported SNMP Versions	36
SNMP Notifications	36
Enable SNMP for an Instance	36
Set Global Instance Monitoring Values	38
Alarms Monitored by RealPresence Platform Director	38
View Active Alarms	40
View Alarms by Entity Type	40
Clear Alarms from the System	41
Viewing and Editing Threshold Values	41
View or Edit Thresholds for a Defined Group	42
View or Edit Threshold Details for a Product Instance	42
View or Edit Threshold Details for a Service Group	42
View or Edit Threshold Details for a Resource Group with a Zone	43
Resource and License Data	43
Available Data	43
Monitored System Resources and License Usage	44
Managing Users	46
User Roles in RealPresence Platform Director	46
System Access by User Type	46
Managing System Users	47
Add a User	47
Edit a User	48
Delete a User	48
Managing Groups	49
Add a Group	49

Edit a Group	50
Delete a Group	50
Managing User Roles	50
Assign Roles to User	50
Add a User Role	51
Edit Permissions for a User Role	51
Delete a User Role	51
Managing Administrator Account Credentials	52
Edit Your Administrator Profile	52
Change Your Administrator Password	52
Managing Platform Settings	53
Managing Certificates	53
Generate Certificates and CSRs	53
View, Copy, or Delete a Certificate	54
Upload a Certificate or Certificate Chain	55
Configure Certificate Settings	55
View and Manage Logs	56
Configure RealPresence Platform Director to use SMTP	57
Enable an SNMP Agent on the RealPresence Platform Director System	58
Upgrade the RealPresence Platform Director System	59
Appendix 1: Network Port Requirements	61
Appendix 2: Troubleshooting	64
Deployment	64
Management	65

Alarm Types	39
Alarm Status Selections	40
RealPresence Platform Director System Access by User Type.	46
Required network ports	61

About This Guide

This Administrator Guide provides the information you need to set up and manage the Polycom® RealPresence® Platform Director™ system and its environment, add RealPresence® Platform® products to it, and license and monitor those products. It assumes that you have completed the installation and initial configuration steps described in the *Polycom RealPresence Platform Director Getting Started Guide*.

Audience, Purpose and Required Skills

This guide is written for a technical audience with knowledge of virtual machine environments, networking, security certificates, software configuration, and videoconferencing.

This guide assumes that you have deployed an instance of the RealPresence Platform Director system.

Downloads

For software downloads, product documentation, product licenses, troubleshooting tips, service requests, and more, visit the [RealPresence Platform Director](#) support site.

Reference Documentation

The following support and reference documentation is available on the [RealPresence Platform Director](#) support site:

- *Polycom RealPresence Platform Director Release Notes*
- *Polycom RealPresence Platform Director Administrator Guide*
- *Polycom RealPresence Platform Director Getting Started Guide*

VMware vSphere support and documentation is available at:

- <https://www.VMware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html>
- <https://my.VMware.com/web/VMware>

Microsoft Hyper-V support and documentation is 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)

Conventions Used in this Guide

This Administrator Guide contains terms, graphical elements, and typographic conventions. Familiarizing yourself with these will help you administer the RealPresence Platform Director system.

Terms Used in this Guide

This guide contains the following Polycom and telecommunications industry terms and acronyms.

Terms used in this guide

Terms	Definition
Apache Tomcat	An open-source web server and application container that runs the web-based RealPresence Platform Director application.
FQDN	Fully Qualified Domain Name. A complete domain name for a computer or host on the internet. Example of an FQDN: dma.example.com.
Hypervisor	Computer software for creating and managing virtual machines (VMs). Microsoft Hyper-V and VMware ESXi are examples of hypervisors.
Hyper-V	Microsoft Hyper-V is a server role for creating and managing a virtualized computing environment in a Windows Server environment. It can create a virtualization platform used to deploy and manage the RealPresence Platform Director and RealPresence Platform Virtual Edition products.
Image	A RealPresence Platform application provided as an Open Virtual Appliance (.OVA) file for VMware or a Hyper-V Export (.ZIP) file for Hyper-V, which is used to create a product instance.
Nginx	An HTTP server used to render static content and delegate requests to Apache Tomcat.
NTP Server	Network Time Protocol Server. An NTP server is needed to synchronize the time and date among RealPresence Platform products.
Provider	VMware vCenter Server is the only currently supported provider. With the correct read and write permissions, the RealPresence Platform Director system can use vCenter APIs to create and manage (start, stop, and delete) virtual instances of RealPresence Platform products. In the absence of a provider, you must create and manage virtual instances using the available hypervisor tools (vSphere or Hyper-V).
Resource Group	In a vCenter environment, a group of computers, storage devices, and network resources that the RealPresence Platform Director system can manage together and to which it can deploy instances. A resource group is created within a zone.
Service Group	An organized collection of virtual instances that work together to make up a video collaboration suite. You can assign instances to a service group in order to monitor and manage them together.
vCenter	The VMware vCenter Server is one product from the vSphere suite. It centralizes the management of multiple ESXi hosts as a single virtual environment. It can be configured as a provider in the RealPresence Platform Director system.
vSphere	VMware vSphere is a suite of products, including VMware ESXi hypervisor, VMware vCenter Server, and other optional products and modules, that create a virtualization platform used to deploy and manage RealPresence Platform Director and RealPresence Platform Virtual Edition products.
Virtual Edition	Designates the software-based virtual machine version of a RealPresence Platform product (as opposed to the hardware-based appliance version).

Terms used in this guide (continued)

Terms	Definition
VM	Virtual machine. A software emulation of a computer, which makes it possible to run multiple operating systems at the same time on one physical computer.
Zone	A RealPresence Platform Director-defined encapsulation of the physical location that houses an instance or set of instances. A zone specifies the time zone and the NTP server(s) for the instances within it. In a vCenter environment, a zone contains one or more resource groups.

Get Help

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

Polycom and Partner Resources

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

- Polycom® RealPresence® Distributed Media Application™ (DMA®)
- Polycom® RealPresence® Resource Manager
- Polycom® RealPresence® Access Director™
- Polycom® RealPresence® Collaboration Server
- Polycom® RealPresence® Media Suite
- Polycom® RealPresence® Web Suite

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

The RealPresence Platform Director system is available in an Appliance Edition (for use with a Polycom Rack Server) and a Virtual Edition, which operates within a VMware vCenter or other supported virtual server environment (VMware vSphere or Microsoft Hyper-V) containing the Polycom RealPresence video system infrastructure.

Polycom RealPresence Platform Director is available as part of Polycom RealPresence Clariti. If you are a RealPresence Clariti customer, you must use the RealPresence Platform Director system to license your products. See [Managing RealPresence Platform Product Licenses](#) for details about license management.

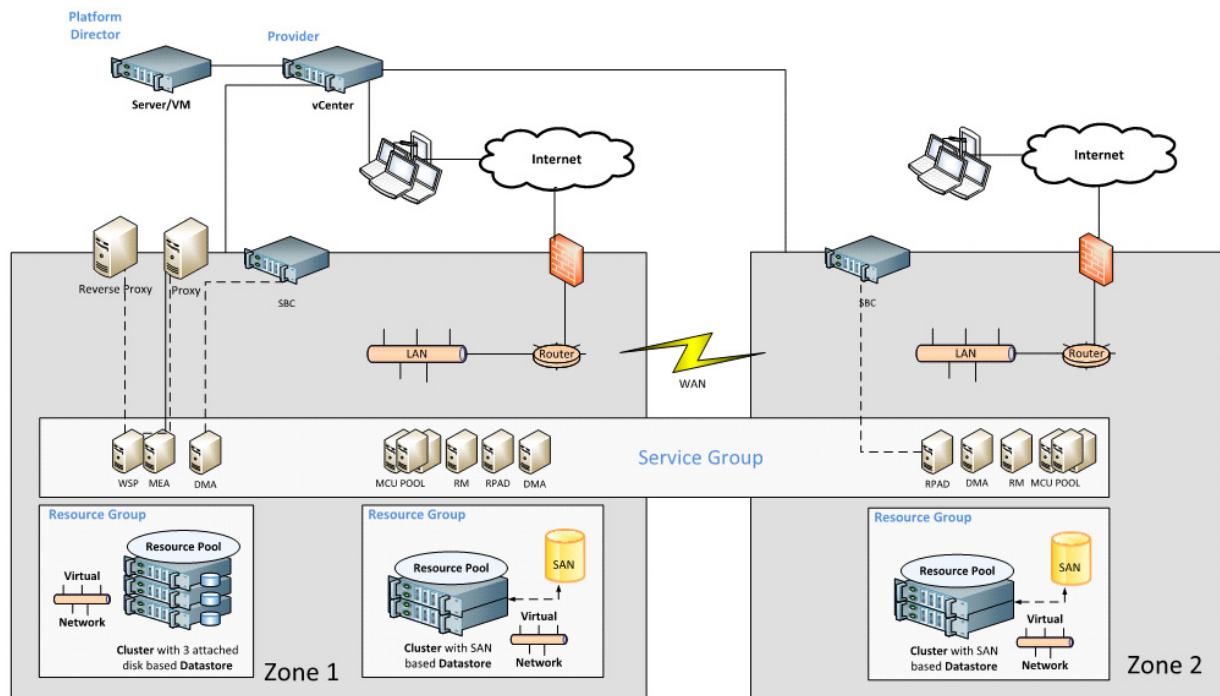
In any supported environment, the RealPresence Platform Director system can monitor RealPresence Platform appliances that do not support RealPresence Clariti. You can add an instance of an appliance to monitor it. See [Add Appliance with Legacy Licensing](#) for details.

Deployment Scenario in A vCenter Environment,

In a vCenter environment, the RealPresence Platform Director system can also (with the proper permissions) create, deploy, and manage (start, stop, and delete) virtual instances of RealPresence Platform products. This versatility enables an administrator to manage all Polycom RealPresence products in one place.

The following graphic illustrates a deployment scenario in an enterprise infrastructure with a vCenter, with data centers distributed globally.

RealPresence Platform Director in a typical network



The vCenter has been added as a provider in the RealPresence Platform Director system. This vCenter controls two data centers, each defined as a zone in the RealPresence Platform Director configuration.

Each zone contains at least one resource group that includes resources such as hosts, clusters, and storage locations.

Instances are placed into service groups in RealPresence Platform Director for easy monitoring by system administrators.

If the RealPresence Platform Director instance is given the appropriate vCenter permissions (see the Appendix 1: Required vCenter Permissions chapter in the *Getting Started Guide*), it can create, delete, and manage virtual instances in the vCenter-controlled data centers. This enables system administrators for this enterprise to create and manage a RealPresence Platform infrastructure across the entire organization with full control over how and where instances are created.

Managing and Configuring the RealPresence Platform Director Environment

The sections that follow describe the configuration of the RealPresence Platform Director environment and the management of its elements. Some apply only to a vCenter environment.

- [vCenter Only: Managing Providers](#)
- [Managing Zones](#)
- [vCenter Only: Managing Resource Groups](#)
- [Managing Service Groups](#)
- [vCenter Only: Managing Virtual Edition Images](#)
- [Adding Instances](#)

vCenter Only: Managing Providers

In a vCenter environment, a provider record specifies the information required to access a vCenter Server, enabling the RealPresence Platform Director system to use the vCenter APIs to create, manage, and monitor virtual RealPresence instances. The RealPresence Platform Director environment must have a provider record for each vCenter Server to which it must connect.

Add a Provider

The provider information includes the URL for the VMware vCenter Server and user account credentials required to create new instances and manage existing ones.

To add a provider:

- 1 Log into the RealPresence Platform Director system as a user with Super Admin privileges.
- 2 Go to **Instance Deployment > Providers** and click **+ PROVIDERS**.
- 3 In the **Add a Provider** page, enter the provider details as outlined in the following table.

Field	Value/Description
Name	A unique name (80 characters maximum) for the provider.
Provider Type	VMware is the only selection available.
URL	The URL for the VMware vCenter Server. The syntax for a VMware provider URL is: <code>https://<vCenter IP address>/sdk</code> In place of the IP address, you can use the fully qualified domain name (FQDN) for the vCenter.

Field	Value/Description
Username	The user ID for accessing the VMware vCenter. See Appendix 1: Required vCenter Permissions in the <i>Getting Started Guide</i> for a detailed description of the vCenter permissions required to enable various RealPresence Platform Director capabilities.
Password	The password for the user.

- 4 Click **ADD** to add the provider.

Edit a Provider

From the **Providers** page, you can select a provider to edit.

To edit a provider:

- 1 Go to **Instance Deployment > Providers**.
- 2 Select the provider you want to edit.
- 3 Click **EDIT**.
- 4 On the **Details** tab, edit the provider information. See [Add a Provider](#) for descriptions of the fields.
- 5 When finished editing, do one of the following:
 - Click **UPDATE** to accept the new field values.
 - Click **RESET** to discard your edits and revert to the existing field values.



Clicking the Update button makes changes permanent. After you have updated details, you cannot use the Reset button to revert to the original values.

Delete a Provider

You can delete a provider when it is no longer applicable to your RealPresence Platform Director configuration. A RealPresence Platform Director system within a vCenter environment requires at least one provider.

To delete a provider:

- » Select the provider you want to delete and click **DELETE**, and follow the instructions in the confirmation dialog.

Managing Zones

A zone is a RealPresence Platform Director concept that helps you configure and manage your Polycom video collaboration environment. It encompasses a time zone, one or more Network Time Protocol (NTP) servers, and in a vCenter environment, one or more resource groups.

The RealPresence Platform Director system associates each virtual machine instance that it manages with a zone.

For a vCenter environment, see [vCenter Only: Managing Resource Groups](#) for information on how to configure and work with resource groups.



At this time, most RealPresence Platform components support only two NTP servers. Because of this limitation, we recommend referencing only two NTP servers for each zone.

Each RealPresence Platform Director system must contain at least one zone in which RealPresence component appliances and virtual instances operate. By default, a new system contains a zone named Default Zone. You can add new ones.

Add a Zone

Each RealPresence Platform Director system must contain at least one zone.

To add a zone:

- 1 Go to **Instance Deployment > Zones** and click **+ ZONE**.
- 2 Enter the zone details, as outlined in the following table.

Field	Value/Description
Name	Enter a name (80 or fewer characters) for the zone.
Description	Enter a brief description (100 or fewer characters) for this zone.
Time Zone	Select the time zone for this zone.
NTP Server	Enter one or more NTP servers for this zone.

- 3 Click **ADD**.
An alert prompts you to add a resource group to the zone. A resource group is necessary only if you are using vCenter. Instances running on an EXSi or Hyper-V host do not require a resource group.
- 4 In a vCenter environment, click **ADD RESOURCE GROUP** to open the Add a new resource group page for this zone. Then, follow the instructions in [Add a Resource Group to a Zone](#) to add a resource group.

Edit a Zone

From the **Zones** page, you can select a zone in order to edit its details, acknowledge or clear alarms, and in a vCenter environment, add or edit resource groups.

To edit details for an existing zone:

- 1 Go to **Instance Deployment > Zones**.
- 2 Select the zone you want to edit.
- 3 On the **Details** tab, edit the zone information.

- 4 When finished editing, do one of the following:
 - Click **UPDATE** to accept the new field values.
 - Click **RESET** to discard your edits and revert to the existing field values.



Clicking the **Update** button makes changes permanent. After you have updated details, you cannot use the Reset button to revert to the original values.

Delete a Zone

You can delete a zone when it is no longer needed. A zone can be deleted only if it contains no resource groups. At least one zone must exist.

To delete a zone:

- 1 Select zone to be deleted.
- 2 Click the **DELETE** button.
- 3 When prompted to confirm, click **YES** to permanently delete the zone.

vCenter Only: Managing Resource Groups

Resource groups are required only in vCenter environments. They provide a way to logically group and effectively manage the available resources.

For example, you may want to deploy compute-intensive and memory-intensive instances on specific clusters or hosts in your vCenter that have ample capacity. You can create one or more resource groups that contain those resources and then monitor them separately to ensure appropriate capacity and performance.

Add a Resource Group to a Zone

A resource group operates within a zone in a RealPresence Platform Director system. You can add a resource group to any defined zone.

To add a resource group to a zone:

- 1 Go to **Instance Deployment > Zones**.
- 2 Select the appropriate zone and click **EDIT**.
- 3 Select the **Resource Groups** tab.
- 4 Click **+ RESOURCE GROUP** to open the **Add a new resource group** page.
- 5 Enter a unique Name and select a provider for the resource group.
The system retrieves the resource information from the vCenter for the selected provider.
- 6 In the **Computer Resource** section, select a **Data Center**, **Host/Cluster**, and **optional Resource Pool** from the lists of those available.
After you select a **Host/Cluster**, the **+ STORAGE** and **+ NETWORK** buttons appear.

7 Click + STORAGE.

The **Add Storage Resources** page lists the available storage resources and the space available on each.

8 Select one or more storage resources and click **ADD.** To select all, click the check box at the top of the column.

9 Click + NETWORK.

The **Add Network Resources** page lists the available virtual networks.

10 Select one or more network resources and click **ADD.** To select all, click the check box at the top of the column.

11 From the **Default Network list, select a default network.** You can select a default network only after choosing at least one network resource.

12 If the data center has folders, and you want to deploy new virtual instances to a folder, enter the folder path in the **Inventory Sub Path field.**

The system appends what you enter to the end of the **Inventory Full Path** entry, which initially contains the name of the data center, followed by /vm. New virtual instances are deployed to the last folder in the full path.


13 Click **CREATE** to add the new resource group to the system.

With a provider, zone, and resource group in place, you can begin adding other RealPresence Virtual Edition products to your vCenter environment.

Edit a Resource Group

As your organization's capacity needs grow, or when you need to take a host out of service for maintenance, you may need to add or remove resources from a defined resource group.

To edit a resource group:


- 1 Go to **Instance Deployment > Zones**.
- 2 Select the appropriate zone, click **EIDT**, and then select the **Resource Groups** tab.
- 3 Click  next to the resource group you want to edit, and then select the **Details** tab.
- 4 Click **Details** to edit the name, storage resources, network resources, or default network. Other details are not editable. For more information, see [vCenter Only: Managing Resource Groups](#).
- 5 Click **Threshold** to enable or disable alarms for CPU utilization, storage, and memory usage, and to edit the threshold values for those alarms.

View Resource Group Status

You can view the status of any resource group in your RealPresence Platform Director environment.

To view the status of a resource group:


- 1 Go to **Instance Deployment > Zones**.
- 2 Select the zone and click **EDIT**.
- 3 Select the **Resource Groups** tab.

- 4 Click  next to the resource group you want to view, and then select the **Status** tab.
After the system initializes, the Status page displays usage information. If you view the status before any data has been collected, the system reports status as in progress.
- 5 Do any of the following:
 - Click the **CPU**, **Memory**, or **Storage** to the left of the graph to change the monitoring information being displayed.
 - At the bottom of the screen, select a time period between 24 hours and 18 months for which you want to view data.
 - Click **STOP** to stop monitoring the resource group data.
 - Click **START** to start or resume monitoring data for the resource group.

Delete a Resource Group

You can delete a resource group that is no longer relevant to your RealPresence Platform Director system. A resource group can be deleted only if it contains no instances.

To delete a resource group:

- 1 Go to **Instance Deployment > Zones**.
- 2 Select the appropriate zone and click **EDIT**.
- 3 Select the **Resource Groups** tab.
- 4 Click  next to the resource group you want to delete, and follow the prompts to complete the deletion.

Managing Service Groups

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

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

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



Include in a service group only virtual and appliance instances that are configured to work together in service of the same RealPresence Platform system, for example RealPresence Collaboration Servers and RealPresence DMA systems. Unrelated sets of instances added into a service group may create invalid monitoring data, or may fail to produce data that is useful in the management of your video collaboration environment.

Create a Service Group

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

To add a new service group to the RealPresence Platform Director system:

- 1 Go to **Instance Deployment > Service Group** and click **+ SERVICE GROUP**.
- 2 Enter a **Name** and **Description** for the new service group.
- 3 Click **ADD** to add the new service group to the list.

After the new service group has been added to the system, you can add the virtual product editions and appliance instances that will operate within it.

View or Edit Service Group Details

You can edit the name and/or description of an existing service group or view details related to it.

To view or edit service group details:

- 1 Go to **Instance Deployment > Service Group** to display a list of available service groups.
- 2 Select the Service Group you want to edit.
- 3 Click **EDIT**.
- 4 Select the **Details** tab, and then click the **Details** row on the left of the screen to open the Service Group details window.
- 5 Update the Name and Description fields as necessary.
- 6 When you have finished editing the service group, do one of the following:
 - Click **UPDATE** to accept all of your new field values, or
 - Click **RESET** to return to all of your previous field values.



Clicking Update makes the change permanent. After you have updated service group details, you cannot use the Reset button to revert to the original field values.

Add a New Instance to a Service Group

You can add a new instance to RealPresence Platform Director through the service group you want it to associate it with.



A service group must contain either a RealPresence DMA system or MCU instance to be shown on the RealPresence Platform Director dashboard.

To add a new Instance to a service group:

- 1 Go to **Instance Deployment > Service Group** to display a list of available service groups.
- 2 Select the Service Group you want to edit.

- 3 Click **EDIT**.
- 4 Select the **Instances** tab, Click **+ INSTANCE** and select one of the following options:
 - **From Common Pool** Select an available instance from the **Add to Service Group** dialog.
 - **Create New Virtual** (vCenter only) Follow the instructions to [Create Instance \(vCenter Only\)](#) from an existing image.
 - **Add Existing Appliance** Follow the instructions to [Add Appliance with Legacy Licensing](#) to the service group.
 - **Add Existing Virtual** (vCenter only) Follow the instructions to [Add Existing Virtual \(vCenter Only\)](#).
 - **Add Existing Virtual by IP** Follow the instructions to [Add Existing by IP](#).
- 5 Click **ADD** to add the instance to the selected Service Group.
The name of the instance now appears in the list of instances for that Service Group.

Remove an Instance from a Service Group

You can remove an instance from a service group at any time. Note that the instance remains available in RealPresence Platform Director after being removed from a service group.

To remove an instance from a service group:

- » Select the instance you want to remove and click **DELETE**.

vCenter Only: Managing Virtual Edition Images

In a vCenter environment where the RealPresence Platform Director system has the appropriate permissions, it can create new virtual machine instances of compatible RealPresence Platform products. To enable that functionality, you must upload the products' Virtual Edition image files.

This section describes how to upload, manage, and delete these image files.

Add a Component Virtual Edition Image

To add an image in RealPresence Platform Director, first download its *.OVA file from the [Polycom Support web site](#) to a local drive until you are ready to upload the image.



Use a Chrome or Firefox browser to upload image files. The file upload APIs in Internet Explorer are not fully supported by the current RealPresence Platform Director software release.

To upload a component virtual edition image:

- 1 Select **Instance Deployment > Image Repository** and click **+ IMAGE**.

2 Enter or select values as outlined in the following table.

Field	Value/Description
Instance Type	Select the Polycom RealPresence component product whose image is being uploaded.
Choose File (*.ova)	Click <input type="button" value="..."/> to browse to the *.OVA file and click Open.
Name	The name is automatically populated based on the name of the image file, but can be changed.
Version	The version number is automatically populated based on the name of the image file, but can be entered manually if necessary. The version of the RealPresence component must be compatible with the RealPresence Platform Director version running in your environment.
Credentials	Select the default credentials (recommended), or select Custom and enter the proper credentials for the system and application users. Custom credentials are not necessary for any products currently supported in the RealPresence Platform Director system. Configuration of virtual machine instances fails if credentials are incorrect.

3 Click **UPLOAD** to begin uploading the image.

Depending on the speed of your network connection and the size of the image file, the upload can take several minutes to an hour or more.



Wait until the image upload is complete before you begin another upload. Do not log out of RealPresence Platform Director or close the browser while the image is uploading; otherwise, the upload fails, and you must delete the image and upload it again.

Edit Image Values

You can edit any of the system values associated with an image.

To edit image values:

- 1 Go to **Instance Deployment > Image Repository** to open a list of available images.
- 2 Select the image to be edited to display the details for the image.
- 3 Edit the **Type**, **Name**, **Version**, or **Credentials** settings for the image. All are required.
- 4 When you have finished editing the image information, do one of the following:
 - Click **UPDATE** to accept the new field values.
 - Click **RESET** to return to the previous field values.

Delete an Image

Delete an image when it is no longer required in your RealPresence Platform Director system.



An image can be deleted only if the RealPresence Platform Director system contains no instances created from it. If an instance exists, the associated image must remain in place.

To delete an image:

- 1 Select **Instance Deployment > Image** Repository.
- 2 In the list of available images, select the image to be deleted.
- 3 Click **DELETE**.
- 4 In the confirmation dialog, click **YES**.

Adding Instances

An instance is a Polycom RealPresence video infrastructure component that runs on a virtual machine or a hardware appliance. When you add RealPresence components to the RealPresence Platform Director solution, it manages licensing and monitors alarms for the components. You can add both virtual or appliance edition products as instances in RealPresence Platform Director.

You add product instances to the RealPresence Platform Director system in several different ways, depending on the product and your environment.

Options	Required Environment	Supported Products
Create Instance Add Existing Virtual	<ul style="list-style-type: none"> • vCenter environment with appropriate permissions 	The following products Virtual Editions are supported: <ul style="list-style-type: none"> • RealPresence DMA • RealPresence Resource Manager • RealPresence Access Director • RealPresence Collaboration Server • RealPresence Web Suite, Experience Portal • RealPresence Web Suite, Service Portal Note that RealPresence Platform Director does not support licensing Polycom RealPresence Media Suite, Virtual Edition in a vCenter environment,

Options	Required Environment	Supported Products
Add Existing by IP	<ul style="list-style-type: none"> • Non-vCenter, • Hyper-V • Appliance editions with RealPresence Clariti licensing 	<p>The following products Virtual Editions are supported:</p> <ul style="list-style-type: none"> • RealPresence DMA • RealPresence Resource Manager • RealPresence Access Director • RealPresence Collaboration Server • RealPresence Web Suite, Experience Portal • RealPresence Web Suite, Service Portal • RealPresence Media Suite <p>The following products Appliance Editions are supported:</p> <ul style="list-style-type: none"> • RealPresence DMA • RealPresence Resource Manager • RealPresence Access Director • RealPresence Media Suite <p>RealPresence Clariti customers who purchase appliance editions of RealPresence Collaboration Server must use the Add Appliance with Legacy Licensing option.</p>
Add Appliance with Legacy Licensing	<ul style="list-style-type: none"> • Appliance edition without RealPresence Clariti licensing 	<p>The following products Appliance Editions can be monitored:</p> <ul style="list-style-type: none"> • .RealPresence DMA • RealPresence Resource Manager • RealPresence Access Director • RealPresence Collaboration Server

Read the following topics on how to adding instances.

- [Create Instance \(vCenter Only\)](#)
- [Add Existing Virtual \(vCenter Only\)](#)
- [Add Existing by IP](#)
- [Add Appliance with Legacy Licensing](#)

Create Instance (vCenter Only)

In a vCenter environment where the RealPresence Platform Director system has the appropriate write permissions (see Appendix 1: Required vCenter Permissions in the *Getting Started Guide*), you can use the RealPresence Platform Director system to create a new instance. When you create an instance of a RealPresence Platform Director component, you configure the network settings for the instance, including the IP address, subnet mask, and gateway to allow users to access the instance on your network. You can also choose to assign those network settings using DHCP.



Creation of a new virtual instance can fail for a variety of reasons, including incorrect application credentials entered for the provider or insufficient resources (disk space or memory) on the host/cluster where the instance is being created.

If a new instance fails to be correctly created and enters an Error state, delete the instance from both the RealPresence Platform Director and the Host/Cluster where the instance was targeted. Resolve the issue before attempting to add the instance again.

When you create a new instance using static IP settings (recommended), have available the following information:

- The IP address (IPv4), subnet mask, and gateway for the new instance.
- The time zone in which you want to run the new instance.



The network settings and time zone options are available only when a new virtual instance is being created. To revise network settings after the instance has been created, log in to the administrator interface for the individual system component, and follow instructions for changing settings as outlined in that product's Administrator Guide.

The RealPresence Platform Director must have at least one defined zone into which you place a new instance. Follow the instructions in [Add a Zone](#) if necessary before creating a new virtual instance.

To create a new virtual instance of a Polycom RealPresence Platform component:

- 1 Go to **Instance Deployment > Instances**.
- 2 Click **+ INSTANCE** and select **Create Instance**.
- 3 On the **Create Instance** page, complete the information in the following table.

Field	Value/Description
Name	Enter a unique name (80 characters maximum) for the instance.
Instance Type	Select the appropriate RealPresence component type from the list.
Image	Select an available image from those listed in the list.
Zone	Select a zone in which the instance will operate.
Resource Group	Select a resource group from those defined in your RealPresence Platform Director environment for the selected zone.
Customize Network & Storage	Select the check box to choose from available storage and network devices.
Service Group	(Optional) Select a Service Group for the instance.
Network Settings	Select one of the two options for assigning an IP address to the instance: <ul style="list-style-type: none"> • Use Static IP • Use DHCP Because some components rely on an IP address that remains constant, Polycom strongly recommends using a static IP, or if you want to use DHCP, reserve a DHCP IP address on your DHCP server for the MAC address of the system component.
Static IP	Enter the IP address for the instance if you opted to use a static IP address.
Subnet Mask	Enter the subnet mask for the IP address.
Gateway	Enter the IP address of the default gateway.

- 4 Click **CREATE** to create the new virtual instance.

The system displays a list of instances being managed or monitored by the RealPresence Platform Director. Depending on the size of the component image and the speed of the network, creating a new virtual instance can take as long as 90 minutes.

View the status field for the new instance to determine the current status: **Creating**, **Powering On**, **Running**, or **Configuring**.

- 5 After a new instance has been created and its status is Running, log into the instance and enable SNMP so that RealPresence Platform Director can monitor it. Follow the instructions for enabling SNMP in the Administrator Guide or Getting Started Guide for that product.
- 6 Then follow the instructions in the [Allocate Licenses for Polycom RealPresence Platform system Components](#) section to allocate license to the instance.

Add Existing Virtual (vCenter Only)

In a vCenter environment where the RealPresence Platform Director system has at least the appropriate read permissions (see Appendix 1: Required vCenter Permissions in the *Getting Started Guide*), you can add an existing instance by pointing the RealPresence Platform Director system to the resource location of the instance (such as its resource group or the host or cluster on which it's deployed).

You can use this procedure to add an existing virtual instance to your RealPresence Platform Director system in the following circumstances:

- To add an older version of a RealPresence Platform system component already running in your virtual data center.
- To add an instance that has been previously created in and then removed from the RealPresence Platform Director system, but not removed from your virtual data center.
- To add an instance that was deployed using VMware tools, rather than through the RealPresence Platform Director system.

To add an existing virtual instance in a vCenter environment:

- 1 Go to **Instance Deployment > Instances**.
- 2 Click **+ INSTANCE** and select **Add Existing Virtual**.
- 3 Provide the appropriate information, as outlined in the following tables.

Field	Value/Description
Instance Type	Select the type of RealPresence Platform component being added.
Image Version	Enter the software version of the instance.
Zone	Select the zone with which to associate the instance. If the instance belongs to a resource group, be sure that the zone contains that resource group.

- If the instance belongs to a resource group, select **Use Existing Resource Group** and complete the information in the following table.

Field	Value/Description
Resource Group	Select the resource group in which the instance is deployed. The list contains the resource groups in the zone you selected. If there are none, or the right one isn't listed, select a different zone.
Instance	Select the instance from the list of instances in the resource group.
Service Group	(Optional) Assign the instance to a RealPresence Platform Director service group.
Application Admin User Name	Enter the administrator user name with which the RealPresence Platform Director system can log into the instance.
Application Admin Password	Enter the password for the administrator user. The credentials must be correct in order for the RealPresence Platform Director system to manage the instance.

- If the instance doesn't belong to a resource group or you don't know, deselect **Use Existing Resource Group** and complete the information in the following table.

Field	Value/Description
Provider	Select the provider (vCenter) that manages the instance being added.
Data Center	Select the data center in which the instance is deployed.
Host / Cluster	Select the host or cluster in which the instance is deployed.
Resource Pool	If the selected host or cluster contains resource pools, select the pool in which the instance is deployed.
Instance	Select the instance from the list of instances in the location you specified.
Service Group	(Optional) Assign the instance to a RealPresence Platform Director service group.
Application Admin User Name	Enter the administrator user name with which the RealPresence Platform Director system can log into the instance.
Application Admin Password	Enter the password for the administrator user. The credentials must be correct in order for the RealPresence Platform Director system to manage the instance.

- 4 Click **ADD** to add the instance to the RealPresence Platform Director system.
Adding, configuring, and licensing an existing instance can take five to fifteen minutes.
- 5 Go back to the **Instances** page to view the list of instances and verify that the instance you added is running.
Next, you can begin allocating licenses for the added instance. See [Allocate Licenses for Polycom RealPresence Platform system Components](#).

Add Existing by IP

You can add existing appliance instances and virtual instances by IP address. Use this option to add virtual editions that you have installed without using RealPresence Platform Director or to add an appliance edition that you want to license and monitor.

Before you add an instance, verify that you are using the correct IP address and that the instance is running and accessible from its own user interface. An instance that is not in a running state will not function correctly when added to the RealPresence Platform Director.

Polycom recommends that SNMP be enabled in any appliance instance before it is added to the RealPresence Platform Director system. Until SNMP is enabled on an appliance instance, that instance will be reported in RealPresence Platform Director as “Not Reachable.”

If you are a RealPresence Clariti customer, use this option for all appliance editions EXCEPT RealPresence Collaboration Server, Appliance Edition.



RealPresence Clariti customers who purchase appliance editions of RealPresence Collaboration Server must use the Add Appliance with legacy license option.

To add an existing instance by its IP address:

- 1 Go to **Instance Deployment > Instances**.
- 2 Click **+ INSTANCE** and select **Add Existing by IP**.
- 3 Provide the information in the following table.

Field	Value/Description
Name	Type a descriptive name (80 or fewer characters) for the instance.
Instance Type	Select the type of RealPresence Platform component being added.
Image Version	Enter the software version of the instance.
Zone	Select the zone with which to associate the instance.
IP Address	Enter the IP address of the instance.
Service Group	(Optional) Assign the instance to a RealPresence Platform Director service group.
Application Admin Username	Enter the administrator user name with which the RealPresence Platform Director system can log into the instance.
Application Admin Password	Enter the password for the administrator user. The credentials must be correct in order for the RealPresence Platform Director system to manage the instance.

- 4 Click **ADD** to add the instance to the RealPresence Platform Director system.
Adding, configuring, and licensing an existing instance can take five to fifteen minutes.

- 5 Go back to the **Instances** page to view the list of instances and verify that the instance you added is running.

Next, you can begin allocating features for the added instance. See [View RealPresence One License Usage Report](#).

Add Appliance with Legacy Licensing

You can add any supported Polycom RealPresence appliance to your RealPresence Platform Director system for monitoring. When you use this option, RealPresence Platform Director does not manage the licensing for the component.

Before you add an instance, verify that you are using the correct IP address and that the instance is running and accessible from its own user interface. An instance that is not in a running state will not function correctly when added to the RealPresence Platform Director.

Polycom recommends that SNMP be enabled in any appliance instance before it is added to the RealPresence Platform Director system. Until SNMP is enabled on an appliance instance, that instance will be reported in RealPresence Platform Director as “Not Reachable.”



RealPresence Clariti customers who use appliance editions of RealPresence Collaboration Server must use the **Add Appliance with Legacy License** option.

To add an existing appliance instance with legacy licensing:

- 1 Go to **Instance Deployment > Instances**.
- 2 Click **+ INSTANCE** and select **Add Appliance with Legacy Licensing**
- 3 Provide the information in the following table.

Field	Value/Description
Name	Type a descriptive name (80 or fewer characters) for the appliance instance.
Instance Type	Select the type of RealPresence appliance instance being added.
Image Version	Enter the software version of the appliance instance.
Zone	Select the zone with which to associate the instance.
IP Address	Enter the IP address of the appliance instance.
Service Group	(Optional) Assign the instance to a RealPresence Platform Director service group.


- 4 Click **ADD** to add the instance to the RealPresence Platform Director system.
- 5 Go back to the **Instances** page to verify that the appliance you added has been added. A successfully added new hardware instance should appear in the list of instances with next to the instance name.


View or Edit Instance Details

You can view information about any instance, including system, error, and network information. You can also view or edit application credentials, SNMP settings, and alarm thresholds.

To view or edit instance details:

1 Go to **Instance Deployment > Instances**.

The Instances list initially shows all instances installed within the RealPresence Platform Director system. Appliance instances are indicated with a hardware icon  next to the instance name.

2 Select the instance that you want to view or edit. To see only a specific type of instance, click , select a type, and click **SEARCH**.

3 Click **EDIT**.

4 Click the **Details** tab, and then do one or more of the following:

- Select **Details** to view or edit detailed information about the instance.
- Select **Credentials** to view or edit the Admin user name for the instance or to change the Admin Username or password. Polycom recommends consulting a member of our support team before editing these fields.
- Select **SNMP** to view or edit the monitoring configuration for the instance.
- Select **Threshold** to view or edit threshold values or enable alarms for resources that are available for monitoring.

5 If you edit information on any of the four pages listed previously, do one of the following:

- Click **UPDATE** to save the new settings.
- Click **RESET TO DEFAULT** to restore default settings.

You must click **UPDATE** to save settings on a page before opening another page. If you move to another page without clicking Update, the new values are not saved.

Delete an Instance

You can delete an instance when it is no longer applicable to your RealPresence Platform Director configuration. When you delete an instance from the RealPresence Platform Director environment, its licenses are automatically allocated back to the pool of available licenses for the system.

To delete an instance:

1 Go to **Instance Deployment > Instances**.

2 Select the instance you want to delete.

3 Click **DELETE**. A dialog prompts you to confirm the deletion.

- If you select **DELETE** instance from MyProvider, a confirmation dialog appears. After you confirm the deletion, the instance is deleted from the RealPresence Platform Director system and the virtual machine is deleted from the vCenter host.
- If you do not select **DELETE** instance from MyProvider, the instance is removed from the RealPresence Platform Director system, but the virtual machine remains available within the host system or vCenter.

Managing RealPresence Platform Product Licenses

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

If you are a RealPresence Clariti customer, you must use the Polycom RealPresence Platform Director system to license your product. RealPresence Platform Director support to manage licenses for the following products that support Clariti:

- Polycom RealPresence DMA, Virtual and Appliance Editions
- Polycom RealPresence Resource Manager, Virtual and Appliance Editions
- Polycom RealPresence Access Director Appliance and Virtual Edition
- Polycom RealPresence Collaboration Server, Virtual Edition
- Polycom RealPresence Media Suite, Virtual and Appliance Edition
- Polycom RealPresence Web Suite, Experience Portal
- Polycom RealPresence Web Suite, Service Portal



To manage licenses with RealPresence Platform Director, you must set it up as a license server in the Polycom Licensing Center, allocate available licenses to it, and then activate those licenses. These tasks are described in the RealPresence Platform Director Getting Started Guide. You should have completed them as part of the initial setup of this RealPresence Platform Director instance. If not, do so before continuing.

- If you have RealPresence Web Suite Services Portal and Experience Portal in your system, you can run those instances one of two ways:
 - Install the instances outside RealPresence Platform Director and manage licenses using their existing license management process.
 - Add the instances to your RealPresence Platform Director system to manage them.

See the *RealPresence Web Suite Administrator Guide* for instructions on how to associate the Services Portal and Experience Portal and set up licensing for those two servers within RealPresence Platform Director.



License features for ContentConnect software Server (Base License for ContentConnect software and High Availability) are displayed on the License Management page as uncounted licenses when you select the Allocation view. The license count shows 0 Instances regardless of how many ContentConnect software instances are available.

RealPresence Platform Director does not display maximum concurrent calls available (Max Number Recorded Calls for ContentConnect software), regardless of whether your organization has purchased a license for those calls.

If you have a RealPresence Clariti solution subscription, you can view or download license usage data for up to 180 days, see [Update the Licenses of Polycom RealPresence Platform system Components](#).

To learn more about RealPresence Clariti, visit <http://www.polycom.com/products-services/realpresence-one.html>.

If your RealPresence Platform components are licensed a la carte, you can use SNMP to monitor resource and license usage on SNMP-enabled instances. See [Monitor the RealPresence Platform Director Environment](#) and specifically [View Resource and License Data](#).

Online and Offline Mode

Licenses for Polycom RealPresence Platform system components can be managed in online or offline mode. If the data center where the RealPresence Platform Director system is located has connectivity to the Internet, you must use online mode to manage licenses. If the data center does not have Internet connectivity, you can manage the RealPresence Platform system components in offline mode.

Allocate Licenses for Polycom RealPresence Platform system Components

The RealPresence Platform Director Getting Started Guide describes setting up the license server and activating RealPresence Platform system licenses within RealPresence Platform Director, and you should already have done that. Now you can allocate licenses for individual components of your RealPresence Platform system. All license allocations for individual RealPresence products are managed through the RealPresence Platform Director **License Management** menu.

A system component must be online, active, and running within the RealPresence Platform Director system before licenses can be successfully allocated to it. In addition, the credentials for the system user configured for the component within RealPresence Platform Director must match the credentials for the system user as configured within the component system.



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

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

To allocate licenses to a RealPresence Platform system component:

- 1 Go to **License Management > Allocation** and do one of the following:
 - Select **Allocate By: Type** to select a product type and see the instances of that type managed by RealPresence Platform Director. Then select a product instance to see a list of applicable licenses and allocate licenses to that specific instance.

- Select **Allocate By: Feature** to see a list of all the activated licenses. Then select a license feature to see the product instances to which that license is applicable and allocate the license feature to specific instances.

For count-based license features (such as max calls), note the number available and set the allocation input field to the number to allocate to the current instance. For uncounted features, set it to 1.

- 2 Click **Save** to save the new license feature allocation.
- 3 Repeat to allocate additional license features to the selected product instance or allocate the selected license feature to additional product instances.
- 4 After allocating licenses, go to the license settings page within each product instance you licensed to verify that the new licenses are available to the product. See the product documentation for instructions on how to view licensing information.



For RealPresence Collaboration Server and RealPresence Access Director products, license allocation changes take effect only after those systems have been rebooted. After either of these products has been installed, RealPresence Platform Director generates an alarm indicating that they must be rebooted.

Update the Licenses of Polycom RealPresence Platform system Components

When you buy additional features or capacity for your RealPresence Platform system components, you must allocate the newly-available licenses to your RealPresence Platform Director license server and activate them within RealPresence Platform Director.

To allocate and activate newly-available licenses:

- 1 In the RealPresence Platform Director management interface, go to **License Management > Setup** and copy the System Identifier number listed on the page.
- 2 In a different browser window, log into the **Polycom Licensing Center** using the URL and credentials sent to you.

See the *RealPresence Platform Director Getting Started Guide* for information about using the **Polycom Licensing Center**.

- 3 Click **Search Servers**, paste the copied system identifier number into the **License Server ID** field, and click **Filter**.

Your RealPresence Platform Director license server appears in the list below.

- 4 Click the license server ID in the list below.

The **View Server** page displays license information for this RealPresence Platform Director license server.

- 5 Click **Map Add-Ons**.

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

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

- 7 In the **Qty to Add** field of the add-ons you want to allocate, enter the number of units to allocate to this RealPresence Platform Director instance and click **Map Add-Ons**.

The **View Server** page returns, displaying a list of the server's licenses. The status for newly-allocated licenses is License not generated. The licenses must be generated (activated within your RealPresence Platform Director system).

- 8 If you allocated too many license add-on units to this RealPresence Platform Director instance and want to remove some, click **Remove Add-Ons**.

The **Remove Add-Ons** page lists the license add-ons available on this instance.

- 9 In the **Quantity to Remove** field of the add-ons you want to change, enter the number of units to remove and click **Remove Add-Ons**.

The **View Server** page returns, displaying a list of the server's licenses. The status for licenses with newly-removed units is Copies decreasing. The removed licenses must be deactivated within your RealPresence Platform Director system.

- 10 If your RealPresence Platform Director instance does not have access to the internet, click **Download Capability Response** to download a local copy of the license file. Note the location of the license file when you download it to your local computer.

If your RealPresence Platform Director system has access to the internet, you must use the online method to license the system and its components. The offline method for managing licenses is not an option when internet access is available.

- 11 Return to the **RealPresence Platform Director License Setup** page, and do one of the following:

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

- 12 Click **UPDATE** to complete the license activation process.

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

For counted licenses, you can now allocate them to the appropriate system component(s), as described in [Allocate Licenses for Polycom RealPresence Platform system Components](#).

View RealPresence One License Usage Report

If your RealPresence Platform is licensed via a RealPresence One solution subscription, the License Report page lets you view or download license usage data for the time period of your choosing (up to 180 days).

To learn more about the RealPresence One solution, visit

<http://www.polycom.com/products-services/realpresence-one.html>.

Every morning at 3:00 AM (server time), the RealPresence Platform Director system retrieves and processes usage data for the preceding 24 hours from the individual components of your RealPresence One solution.



The call detail records (CDRs) for a call aren't available until the call ends, and CDRs are retrieved at 3:00 AM, not midnight.


To generate a license report for Day 1, the system includes all calls with either a start time or an end time between 3:00 AM on Day 1 and 3:00 AM on Day 2, including calls that ended between 3 AM on Day 1 and 3:00 AM on Day 2 (but not calls that span more than two days).

For instance, the data for Day 1 include Day 1 calls that end on Day 2, which are retrieved and processed at 3:00 AM on Day 3. Consequently, the most recent usage information available is always for two days earlier.

For each day in the date range you specify, the report shows the maximum level (high-water mark) for concurrent calls, concurrent connection license usage, and user license usage. You can use this information to determine if your RealPresence Platform system is nearing its licensed capacity and may need more license elements of a specific type.

The system stores up to 18 months of usage data.

To create a license usage report:

- 1 Go to **License Management > Report**.
- 2 Click  to set the start and end dates of the date range you want the report to cover.
- 3 Click **Search**.
The system generates the report. Depending on the date range you requested, this may take some time.
- 4 Click **Export** to download a .csv (comma-separated values) file of the report, which you can open in Excel or another spreadsheet application.

The report contains a line for each date in the range. The following table describes the fields in the report.

Field	Value/Description
Max Total Calls	The maximum number of concurrent total calls, point-to-point and multipoint (conference), at any time on the specified date. This is informational, not a licensed value. It provides an indication of how busy your system gets at peak times.
Max P2P Calls	The maximum number of concurrent point-to-point calls at any time on the specified date. This is informational. Point-to-point calls don't use a call license, but the number of concurrent point-to-point calls is limited to the number of User licenses purchased.
Max Standard Connection	The maximum number of Standard Concurrent Connection licenses in use at any time on the specified date. Every endpoint, software client, or user device joining a conference call consumes a Concurrent Connection license. Conference calls are also known as VMR (virtual meeting room) calls. A Standard Connection license supports SVC up to 720p, AVC up to CIF, and VoIP calls.

Field	Value/Description
Max Universal Connection	<p>The maximum number of Universal Concurrent Connection licenses in use at any time on the specified date.</p> <p>A Universal Connection license supports all resolutions and advanced functions available, including full AVC support and support for H.323 calls, ITP, and TIP. It can be used in place of a Standard Connection license when no more of those are available.</p>
Max Users	<p>The maximum number of User licenses in use at any time on the specified date.</p> <p>Every registered user and video conferencing device not assigned to a user (such as a room system) consumes a User license.</p>

Monitoring the RealPresence Platform Director Environment

The RealPresence Platform Director system uses Simple Network Management Protocol (SNMP) to monitor instances of Polycom RealPresence products that support SNMP monitoring. An instance must be in a Running state with SNMP enabled to be monitored in RealPresence Platform Director.

In addition, the RealPresence Platform Director system itself can be monitored via SNMP. See [Enable an SNMP Agent on the RealPresence Platform Director System](#).

SNMP Description

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of resources in a network.

SNMP Framework

The SNMP framework has three parts:

- **An SNMP manager** 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. The RealPresence Platform Director system acts as an SNMP manager for the RealPresence Platform instances that it's configured to monitor.

The SNMP agent on the instance to be monitored and the RealPresence Platform Director 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's configured to communicate. To monitor the RealPresence Platform Director system itself, you configure an SNMP agent on the system to communicate with a third-party SNMP manager, such as Nagios.

The RealPresence Platform Director SNMP agent and the SNMP manager to monitor it must have matching SNMP configurations in order for them to communicate.

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

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. Traps are less reliable because the SNMP manager does not send any acknowledgment when it receives a trap. Traps are sent only once, and the SNMP agent discards traps as soon as they are sent.
- Inform requests (informs) are traps that include a request for a confirmation of receipt from the SNMP manager. The agent holds an inform request in memory until it receives a response or the request times out. 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.

Enable SNMP for an Instance

Enabling SNMP for an instance configures the RealPresence Platform Director system to act as an SNMP manager for that instance, receiving communications from an SNMP agent on the instance. You must enable SNMP on each RealPresence Platform component instance that you want to monitor. Then you can configure SNMP settings for the instance in the RealPresence Platform Director system.

Most SNMP manager settings are set only at the instance level. See [Set Global Instance Monitoring Values](#) for the two exceptions.

You can implement one of the following SNMP versions:

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



For each RealPresence Platform component instance that you want to monitor, the instance monitoring configuration in the RealPresence Platform Director system must match the SNMP configuration of that instance.

To configure SNMP settings for monitoring an instance:

- 1 Go to **Instance Deployment > Instances**.
- 2 On the **Instances** screen for the instance you are editing, click **EDIT**.
- 3 Select the **Details** tab, and then click **SNMP** at the left of the screen.
- 4 Select the SNMP version.
The configuration selections vary depending on which SNMP version you choose.
- 5 Depending on the SNMP version selected, complete the applicable fields of the instance monitoring configuration, described in the following table.

Field	Value/Description
Transport	The transport protocol to be used. At this time, RealPresence Platform Director supports only UDP (User Datagram Protocol), not TCP. 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 manager communicates.
Community	For SNMPv2c only. Functions as a global password for accessing SNMP information on the instance. The instance must be configured with the same community string in order for the SNMP manager to communicate with it. Per SNMP convention, the default community string is "public", but this should 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 Type	Specifies the authentication protocol. These protocols are used to create unique fixed-sized message digests of a variable length message. Possible values for authentication protocol are: <ul style="list-style-type: none"> • MD5—Creates a digest of 128 bits (16 bytes). • SHA—Creates a digest of 160 bits (20 bytes). Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.
Authentication Password	For SNMPv3 only. Specifies the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest.

Field	Value/Description
Encryption Type	<p>For SNMPv3 only.</p> <p>Specifies the privacy protocol for the connection between the RealPresence Platform Director system and the SNMP agent.</p> <p>The RealPresence Access Director system implements communication with authentication and privacy (the authPriv security level as defined in the USM MIB).</p> <p>Possible values for privacy protocol are:</p> <ul style="list-style-type: none"> • DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet.
Encryption Password	<p>For SNMPv3 only.</p> <p>Specifies the password to be associated with privacy protocol.</p>

- 6 Click **UPDATE** to save the new settings.

Set Global Instance Monitoring Values

Most SNMP manager settings are set at the instance level (see [Enable SNMP for an Instance](#)). The two exceptions are set on the **MONITORING** page, and they specify how long the SNMP manager waits for a response to a query and how many times it retries. These values apply to all instances being monitored.

To set global instance monitoring values:

- 1 Go to **Admin > Application Settings**.
- 2 Click **MONITORING** and change, if necessary, the settings described in the following table.

Field	Value/Description
Retry Count	Specifies the number of times the SNMP manager retries a query to a monitored instance. Valid values are 2 through 5. The default is 2.
Timeout	<p>Specifies how long (in milliseconds) the SNMP manager waits for a response from a monitored instance before retrying the query. Valid values are 1000 through 10000. The default is 1500.</p> <p>Set a higher timeout value if the RealPresence Platform Director system is far away from one or more of the instances that it monitors.</p>

- 3 Click **UPDATE** to save the new settings.

Alarms Monitored by RealPresence Platform Director

You can view the current state of alarms monitored by the RealPresence Platform Director on the **ALARMS** page. The initial **ALARMS** page shows all alarms across Instances, Resource Groups, Service Groups, Zones, Providers, and unified management.



A RealPresence Platform Director instance may experience various failure conditions when a host or cluster executing RealPresence Platform Director becomes overloaded. If unexplained failure conditions occur in RealPresence Platform Director, check the configuration of the host system or vCenter to determine whether an overloaded host or cluster may be the cause of failures.

The Unresolved Alarms box in the upper-right corner of the Alarms window provides a color-coded view of the number and severity of the alarms. The alarm colors correspond to the following threshold levels:

- **Gray** System has reached the Warning Value threshold.
- **Yellow** System has reached a one-third increase in percentage between the Warning and Critical values.
- **Orange** System has reached a two-thirds increase in percentage between the Warning and Critical values.
- **Red** System has reached the Critical Value threshold.

Alarms included in the RealPresence Platform Director system are outlined in the following table.

Alarm Types

Alarm Type	Description	Corrective Action
Configuration Alarm	A problem was detected during the configuration phase that involves either creating a new instance or adding an existing instance.	Typically, this is a problem with the application credentials. Delete the instance from RealPresence Platform Director, and then add it again using the correct credentials.
License Change Alarm	The system has detected a change in licensing status for a product that requires a reboot of the system.	Reboot or restart the affected system.
System Reachability Alarm	A system entity is unreachable by the RealPresence Platform Director. The entity may be a provider, resource group, or an instance that may have been powered off, given a new IP address, or deleted from the vCenter.	Either delete or power up the entity.
Provider Login Failure Alarm	A login failure prevented a connection to the Provider. This may have happened if the system credentials were changed in the affected instance but not in RealPresence Platform Director.	Add the correct application credentials to the Provider details.
Total CPU Usage	Generated when a CPU threshold has been reached.	Refer to documentation for the entity initiating the alarm.
Memory Usage	Generated when a memory threshold has been reached.	Refer to documentation for the entity initiating the alarm.
Storage Disk Usage	Generated when a disk storage threshold has been reached.	Refer to documentation for the entity initiating the alarm.

(continued) Alarm Types

Alarm Type	Description	Corrective Action
Video Ports Usage	Generated when an application threshold for video port usage has been reached.	Allocate more licenses to the entity.
Voice Ports Usage	Generated when an application threshold for voice port usage has been reached.	Allocate more licenses to the entity.
NW Interface Usage	Generated when a disk storage threshold has been reached.	Refer to documentation for the entity initiating the alarm.

View Active Alarms



The default view shows all alarms that are active in the system. You can filter the view to show alarms by **Instance**, **Resource Group**, **Zone**, **Service Group**, or **Provider**.

Selections for viewing alarms are defined in the following table.

Alarm Status Selections

Field	Value/Description
Show Active	Alarms that have occurred that have not been cleared. Both New and Acknowledged alarms are displayed.
Acknowledged	Marks an alarm as being grayed out on the Show Active alarm; indicates that an admin is aware of the alarm.
New	Alarms that are active but not yet acknowledged.
Cleared	Alarm condition has been resolved.

To view active system alarms:



- 1 Go to **Alarm > Alarms** to display a list of current alarms.
- 2 Click **CLEAR** or **ACKNOWLEDGE**.
- 3 Click .
- 4 Click the **Show Active** field and select **New**, **Acknowledge**, or **Cleared** to filter the alarms you want to clear or acknowledge.
- 5 Select  at the right to show details about the selected alarms.

View Alarms by Entity Type

You can view alarms in groups by entity type, including by Instance, Resource Group, Zone, Service Group, or Provider.

To view Alarms for any entity:

- 1 Go to **Alarm > Alarms** to display a list of current alarms.

- 2 Click  .
- 3 Click the **Type** field and select one of the following entity types:
 - **INSTANCE** View alarms related to RealPresence Platform Director component instances.
 - **RESOURCE GROUP** View alarms related to Resource Groups.
 - **ZONE** View alarms related to Zones.
 - **SERVICE GROUP** View alarms related to Service Groups.
 - **PROVIDER** View alarms related to a Provider.
- 4 Select the status of the alarms you want to show, as follows:
 - **Show Active** Show all active alarms.
 - **New** Show only new alarms.
 - **Acknowledged** Show only acknowledged alarms.
 - **Cleared** Show only cleared alarms.
- 5 Click  next to any displayed alarm to show further details about the alarm.

Clear Alarms from the System

You can clear alarms for **Providers**, **Zones**, **Instances**, or **Service Groups**. To clear any alarm, start at the **RealPresence Platform Director** page for that entity, and select the available entity for which you want to clear an alarm.

To clear an active alarm:

- 1 Go to one of the following:
 - **Instance Deployment > Providers**
 - **Instance Deployment > Zones**
 - **Instance Deployment > Instances**
 - **Instance Deployment > Service Group**
- 2 Select the **Provider**, **Zone**, **Instance**, or **Service Group** whose alarm you want to edit.
- 3 Click the **Details** tab.
- 4 Click the **Alarms** tab.
- 5 Select the check box next to the alarm you want to clear, and select either **ACKNOWLEDGE** or **CLEAR** from the Actions list.

After you acknowledge or clear an alarm, it is removed from the active alarms list. You can review the alarm by selecting the appropriate option from the **Show Active** list.

Viewing and Editing Threshold Values

You can view the current default threshold values for RealPresence Platform Director alarms for each product. When a monitored metric exceeds a threshold, an alarm is raised. Thresholds are set to default values for RealPresence Platform Director product groups but can be changed within individual product instances.

View or Edit Thresholds for a Defined Group

You can view and edit Threshold values for **Instances**, **Zones**, or **Resource Groups**. Resources available for editing depend upon entity type.

To view or edit alarm thresholds for Instances in a RealPresence Platform Director product group:

- 1 Go to **Alarm > Threshold** to display details for each of the installed RealPresence Platform Director system products.
- 2 Click one of the component types listed in the rows at the left of the screen.
The Resources column displays the resources that are available and being monitored for the selected component.
- 3 Change applicable **Critical Value in %** and **Warning Value in %** fields for each resource on the selected component.
- 4 Select or clear the **Enable Alarm** check box to control whether RealPresence Platform Director shows the alarm for the given resource threshold.
- 5 Click **UPDATE** to save the new alarm threshold values.

View or Edit Threshold Details for a Product Instance

You can view and edit threshold details for any individual product instances.

To view or edit threshold details for a specific product Instance:

- 1 Go to **Instance Deployment > Instances** to edit threshold details for a specific instance.
- 2 Select the instance whose details you want to edit.
- 3 Click **EDIT**.
- 4 Click the **Details** tab, and then click **Threshold** at the left of the screen.
The same data fields are shown for both hardware and software Instances.
- 5 Update the threshold information for any of the following resources: **CPU utilization**, **Storage**, **Memory**, **Network**, **Video Ports**, or **Audio Ports**.
- 6 Do one of the following:
 - Click **UPDATE** to set the new values.
 - Click **RESET TO DEFAULT** to return the values to the system defaults.

View or Edit Threshold Details for a Service Group

Threshold details are available for any service group that has been defined within your RealPresence Platform Director system. You can view and edit details for the entire group.

To edit Threshold details for a Service Group:


- 1 Go to **Instance Deployment > Service Group**.
- 2 Select the service group whose details you want to edit.

- 3 Click **EDIT**.
- 4 Select the **Details** tab, and then click **Threshold** at the left of the screen.
- 5 Change the warning values for any available resource, and select the **Enable Alarm** check box to enable the alarm for that resource.
- 6 Do one of the following:
 - Click **UPDATE** to set the new values.
 - Click **RESET TO DEFAULT** to return the values to the system defaults.

View or Edit Threshold Details for a Resource Group with a Zone

You can view and edit Threshold values for resource groups within a zone.

To edit Threshold details on a Resource Group within a Zone:

- 1 Go to **Instance Deployment > Zones**.
- 2 Select the zone whose details you want to edit.
- 3 Click **EDIT**.
- 4 Select the **Resource Groups** tab, and then click  next to the appropriate resource group.
- 5 Select the **Details** tab, and then click **Threshold** at the left of the screen.
- 6 Change the warning values for any available resource, and select the **Enable Alarm** check box to enable the alarm for that resource.
- 7 Do one of the following:
 - Click **UPDATE** to set the new values.
 - Click **RESET TO DEFAULT** to return the values to the system defaults.

Resource and License Data

You can view the operational status of system resources by **Resource Group**, **Instance**, or **Service Group** for entities with SNMP enabled.



If your RealPresence Platform is licensed via the RealPresence One solution subscription, RealPresence Platform Director's License Report feature is enabled. See [View RealPresence One License Usage Report](#).

Available Data

Monitored system resources include CPU, memory, storage, and network. RealPresence Platform Director also monitors and displays your system's usage of licensed features that have been purchased and allocated to the Polycom RealPresence instances that are managed by your RealPresence Platform Director. Graphs show system usage for both resources and licensed features along with minimum, maximum, and average capacity over the selected time period.

License usage information is available in the Instance view; it is not available for Resource or Service Groups. See the Administrator Guide for the specific RealPresence product for descriptions of the licensed features that can be allocated for it.

For resources and license features being monitored other than those for RealPresence Resource Manager, you can select data from the following time periods: 24 hours, 1 month, 3 months, 6 months, 12 months, or 18 months. RealPresence Resource Manager usage information is available only for the preceding 24 hours.


Monitored System Resources and License Usage

Resource and License Data available for each monitored RealPresence product is outlined in the following table. Note that because RealPresence CloudAXIS Experience Portal and Services Portal do not support SNMP, system resource and license information is not available for those products. For a list of the notifications sent by the RealPresence Web Suite and Web Suite Pro Services Portal, see “SNMP Notifications” in the RealPresence Web Suite Administrator Guide.

Monitored System Resources and License Usage

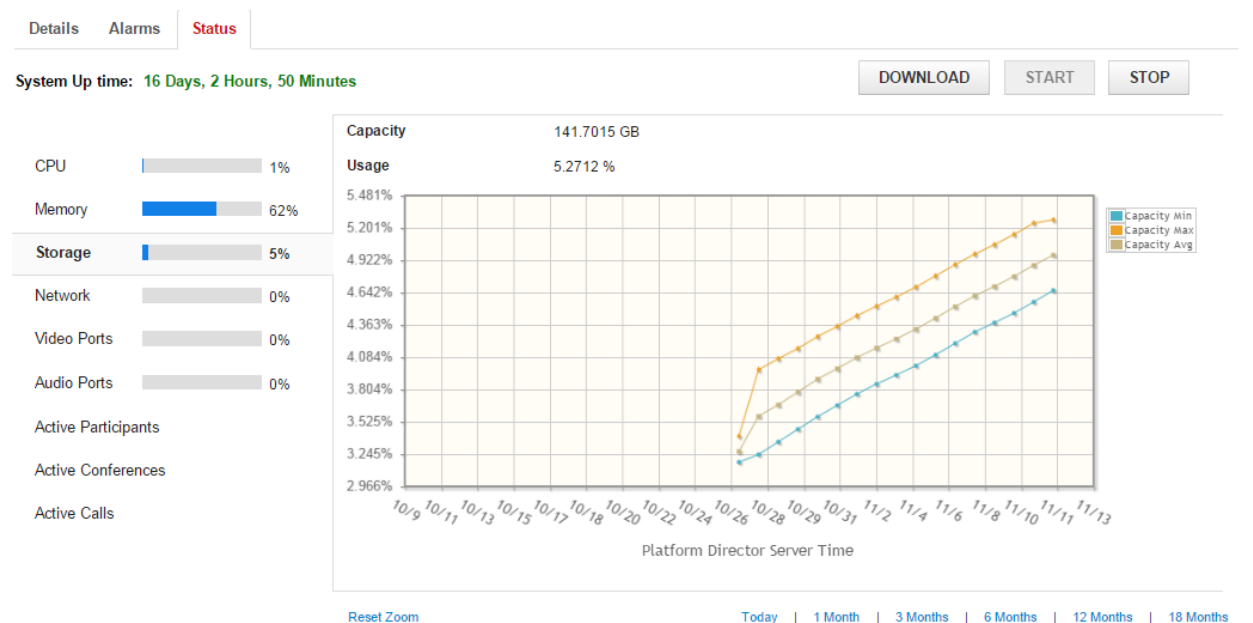
Resource/License	RealPresence Access Director	RealPresence Collaboration Server	RealPresence Resource Manager	RealPresence DMA
CPU	Yes	Yes	Yes	Yes
Memory	Yes	Yes	Yes	Yes
Storage	Yes	Yes	Yes	Yes
Network	Yes	Yes	Yes	Yes
Call Service	Yes	No	No	No
Active Calls	Yes	No	No	No
Video Ports	No	Yes	No	Yes
Audio Ports	No	Yes	No	Yes
Active Participants	No	Yes	No	Yes
Active Conferences	No	Yes	No	Yes
Active Calls	No	No	No	Yes
Active Audio Calls	No	Yes	No	No
Active Video Calls	No	Yes	No	No
Used Ports	No	Yes	No	No
Completed Adhoc Conferences	No	No	Yes	No
Active Adhoc Conferences	No	No	Yes	No
Active Scheduled Conferences	No	No	Yes	No
Future Scheduled Conferences	No	No	Yes	No
Managed Endpoints	No	No	Yes	No

To view system resource and/or license data for a Resource Group, Instance, or Service Group:

- 1 Go to one of the following:
 - **Instance Deployment > Instances** to select a specific instance.
 - **Instance Deployment > Service Group** to select a service group.
 - **Instance Deployment > Zones** to select a Zone, and then select the **Resource Groups** tab to display a list of available Resource Groups.
- 2 Select the instance, service group, or resource group whose status you want to view.
- 3 Click **EDIT** or  next to the selected resource group.
- 4 Select the **Status** tab to view usage information for available monitoring data. Data available depends upon the type of entity you have selected, as shown in the preceding table.
- 5 Do any of the following:
 - Select the tabs to the left of the graph to change the information being displayed.
 - At the bottom of the screen, select a time period between 24 hours and 18 months for which you want to view data. This option is not available for RealPresence Resource Manager, which provides usage information only for the preceding 24 hours.
 - Click **DOWNLOAD** to download a .csv file containing the raw data displayed in the graph.
 - Click **STOP** to stop monitoring the selected data.
 - Click **START** to resume monitoring.

The instance details screen shows the resources and license features being monitored by the system for that instance, as shown in the following screen example.

Instance Status Screen



Managing Users

The sections that follow provide information for managing users of the RealPresence Platform Director system. Users are created and managed locally and comprise various types of system administrators.

This section includes information on managing users, groups, and roles within the RealPresence Platform Director system.

User Roles in RealPresence Platform Director

Available user roles are described in the table below.

RealPresence Platform Director System Users

User Role	Access granted in RealPresence Platform Director
Administrator Permissions	This user role has the highest privileges and permits the administrator to perform all system configurations and manage all data centers housed within RealPresence Platform Director vCenter or host system. Only roles with Administrator Permissions can add, delete, or edit users.
Data Center Management Permissions	This user role is intended for a data center administrator who can choose to add, edit, and remove resources being used inside a zone. This role has the ability to arrange instances within a data center to optimize available resources.
Video Network Management Permissions	This user role is intended for an administrator responsible for maintaining a Service Group. The administrator can add images and create or delete instances from Service Groups as required.
Auditor Permissions	This user can read, but not edit, the system configuration. This user type is intended for someone responsible for monitoring the system and reporting issues.

System Access by User Type

The level of access each user type has to the RealPresence Platform Director system is outlined in the following table.

RealPresence Platform Director System Access by User Type

User Task	Administrator	Data Center Management	Video Network Management	Auditor
Alarms	Read/Write	Read/Write	Read/Write	Read
Thresholds	Read/Write	Read	Read	Read

(continued)RealPresence Platform Director System Access by User Type

User Task	Administrator	Data Center Management	Video Network Management	Auditor
Download logs	Yes	Yes	Yes	Yes
User management	Read/Write	No access	No access	No access
Instance operations	Read/Write	Read	Read/Write	Read
Service Groups	Read/Write	Read	Read	Read
Resource Groups	Read/Write	Read	Read	Read
Images	Read/Write	Read	Read/Write	Read
Zones	Read/Write	Read	Read	Read
Start/stop monitoring	Yes	Yes	Yes	No
System settings	Read/Write	Read*	Read*	Read*

*All of these have read access to logs and Application settings (Monitoring and SNMP) but nothing else under SETTINGS.


Managing System Users

The **USERS** page offers a view of system users and their assigned roles. From this page, you can add, edit, and delete users from the RealPresence Platform Director system.

Add a User

Only Admin users can add other users to the system. Any time RealPresence Platform Director is configured with SMTP settings, the user password is always emailed to the new user.

To add a user:

- 1 Go to **User Management > Users**.
- 2 Click  to open the **Add New user** dialog. The **User Enabled** option is selected by default.
- 3 Enter the following information. Fields marked with * are required.

Column	Description
First Name	The user's first name
Last Name	The user's last name
User ID	The user's unique login name. This user ID must be unique across all domains.
Password	The user's assigned password. This password must be a minimum of eight characters in length.
Email Address	The user's email address. (The email address is an ASCII-only field.)



Column	Description
Contact Number	The user's phone number.
Title	The user's professional title.
Department	The user's department within the enterprise.
City	The city in which the user's office is located.

- 4 (Optional) Click the **Create Password** button to generate a password by the system. After you click **Create Password**, you will see the password on the Confirm Password dialog. Remember the password and click **OK**.
- 5 Click **Save** to create the user.
- 6 In the **Associated Roles** section, select and move the required role(s) to **Selected Roles** list. Move the unwanted role(s) to the **Available Roles** list.
- 7 Click **Save** to save the changes.

Edit a User

An administrator user can edit details for any user of the RealPresence Platform Director system.

To edit User details:

- 1 Go to **User Management > Users**.
- 2 Search the user by clicking .
- 3 Enter the user's first name, last name, user ID, or domain to search the user to edit.
- 4 If the list is too large to scan, further refine your search string.
- 5 Select the user of interest and click .
- 6 On the **Edit User** dialog, do one of the following:
 - Click in the appropriate text box to edit the details you want to edit.
 - Enable or disable the user by selecting or clearing the **Enable User** check box.
- 7 Click **Save** when you complete all edits.





If you do not have SMTP settings configured in the Platform Settings section, the user will not receive notification of a changed password. For information on configuring SMTP settings, see [Configure RealPresence Platform Director to use SMTP](#).

Delete a User

You can delete only local users from the RealPresence Platform Director system. You cannot delete users added through integration with an enterprise directory.

To delete a user:

- 1 Go to **User Management > Users**.
- 2 Search the user by clicking .

- 3 Enter the user's first name, last name, user ID, or domain to search the user to edit.
- 4 If the list is too large to scan, further refine your search string.
- 5 Select the user of interest and click  .
- 6 Click **OK** to confirm the deletion.

The user is deleted from the RealPresence Platform Director system.


Managing Groups

In the RealPresence Platform Director system, only users assigned the **Administrator Permissions** role can management groups.

Add a Group

You can add local groups.

To add a group:

- 1 Go to **User Management > Groups**.
- 2 Click  to open the **Add Group** dialog.
- 3 Enter the information under the **General Info** tab as shown in the table below.
- 4 Click **Update** to create the group.
- 5 Enter the information under the Associate Roles, Group Members, and Address Book tabs as shown in the following table. You can edit these information only after create a group by clicking **Update**.
- 6 Click **Update** again to save the changes.


Field	Value/Description
General Info	
Group Name	A meaningful and unique group name assigned when creating the group.
Description	A more complete description of the group's purpose
Enterprise Directory Viewable	Whether or not the group is displayed in the endpoint directory
Associated Roles	
Available Roles	The list of roles defined to the RealPresence Platform Director system.
Selected Roles	The list of roles that you assign users when adding them to the system. Users have all of the permissions associated with all of the roles assigned to them (that is, permissions are cumulative).
Group Members (Local Users Only)	
Search Available Members	Search field for finding users

Field	Value/Description
Search Results	The users and groups identified to the system that you can add to the local group. This list can include both local and enterprise users and groups.
Group Members	The users and groups selected as part of the group
Address Book	
Address Book	Select the address book to assign it to this group.

Edit a Group

You can edit groups.


To edit a group:

- 1 Go to **User Management > Groups**.
- 2 In the Groups page, select the group of interest and click .
- 3 As required, edit the **General Info**, **Associated Roles**, **Group Members**, and **Address Book** sections.
- 4 Click **OK**.

Delete a Group

You can delete a local or enterprise group.

To delete a local or enterprise group:

- 1 Go to **User Management > Groups**.
- 2 In the Groups page, select the group of interest and click .
- 3 Click **OK** to confirm the deletion.


Managing User Roles

In the RealPresence Platform Director system, only users assigned the **Administrator Permissions** role can manage user roles.

Assign Roles to User

You can assign one or more roles to a user.

To assign roles to a user:


- 1 Go to **User Management > Users**.
- 2 Search and select the user of interest and click .

- 3 In the **Associated Roles** section, select and move the required role(s) to **Selected Roles** list. Move the unwanted role(s) to the **Available Roles** list.
- 4 Click **OK**.

Add a User Role

When you add a user role, you also specify permissions for the role.


To add a user role:

- 1 Go to **User Management > User Roles**.
- 2 Click  to open the **Role Add** dialog.
- 3 Complete the **Name** and **Description** fields of the **Role Add** dialog.
- 4 Click **Update** to create the role.
- 5 Click Platform Director Permissions and assign permissions to the new role by selecting the roles. See [User Roles in RealPresence Platform Director](#) for details about role description.
- 6 Click **Update**.

Edit Permissions for a User Role

You can change permissions for the default roles, as well as for other user roles that were created manually.


To edit the permissions for a user role:

- 1 Go to **User Management > User Roles**.
- 2 As needed, use the Filter to customize the User Roles list.
- 3 In the User Roles list, select the role of interest and click .
- 4 Edit the Description field of the Role Edit dialog and edit permissions for the role.
- 5 Click **Update**.

Delete a User Role

You can delete a user role from the RealPresence Platform Director system if no users are currently assigned to it.

To delete a user role:

- 1 Go to **User Management > User Roles**.
- 2 As needed, use the Filter to customize the User Roles list.
- 3 In the User Roles list, select the role of interest and click .
- 4 Click **OK** to confirm the deletion.

Managing Administrator Account Credentials

You can edit or change your user account credentials after logging in to the RealPresence Platform Director. Access your account settings through the Admin list in the upper-right corner of the RealPresence Platform Director page to change either your user profile or password.

Edit Your Administrator Profile

To edit your user profile:

- 1 From the **Admin** menu list, select **Edit Profile**.
- 2 Make the necessary changes in the profile settings
Note that the **Email Address** field is required.
- 3 Click **UPDATE**.

Change Your Administrator Password

You are required to change your password after logging in for the first time, but you can also change your password at any time through the Account Settings list.

To change your password:

- 1 From the **Admin** menu list, select **Change Password** to open the **Change Password** dialog.
- 2 Type your current password and a new password, and retype the new password.
- 3 Click **CHANGE** to change your password.
- 4 Sign out and return to the login screen to log into RealPresence Platform Director with your new credentials.

Managing Platform Settings

In the **Platform Settings** page of RealPresence Platform Director, you can configure specific settings for the platform and for specific applications.

Managing Certificates

RealPresence Platform Director requires the use of Secure Socket Layer (SSL) connections to access its user interface. When a browser establishes a secure connection with RealPresence Platform Director, it receives a certificate identifying the RealPresence Platform Director server. The browser uses this certificate, which may be self-signed or signed by a third party Certificate Authority (CA), to determine whether the server is safely and securely accessed.

This section shows you how to complete the following tasks:

- [Generate Certificates and CSRs](#)
- [View, Copy, or Delete a Certificate](#)
- [Upload a Certificate or Certificate Chain](#)

While self-signed certificates provide encryption for SSL connections, they are less secure than certificates signed by a CA. Most browsers display warning messages and advise against accessing any site that uses a self-signed certificate. To avoid these warnings without compromising your browser security, you can either import the self-signed certificate as a trusted certificate into your web browser, or use a certificate signed by a CA to identify the RealPresence Platform Director server.

To use a certificate signed by a CA, you must do the following:

- Generate a certificate signing request (CSR).
- Submit that request to a CA (either local to your organization or public).
- Upload the signed certificate received from the CA to the RealPresence Platform Director, along with the certificate's trust chain.

Generate Certificates and CSRs



This section describes how to either generate a self-signed certificate or generate a CSR that can be sent to a third-party CA. For details on uploading certificates, see [Upload a Certificate or Certificate Chain](#).



Verify that a new certificate or CSR is necessary before following this procedure. Generating a new certificate or CSR overwrites the previous one.

To generate a certificate or CSR:

- 1 Go to **Admin > Platform Settings**. Then click **CERTIFICATE**.
- 2 On the **SETTINGS** page, click the **Generate CSR/Certificate** tab to display the CSR/Certificate settings.
- 3 Enter information in the fields as shown in the following table.

Field	Value/Description
Operation Type	Choose one of the following options from the list: <ul style="list-style-type: none"> • CSR – Generates a Certificate Signing Request • Certificate – Generates a self-signed certificate
Type	WebServer is the only available type.
Organization	The name of your organization.
Organizational Unit	Any details that help identify the entity requesting the certificate.
Country	The two-letter ISO code for the country in which your organization operates.
State	List the full state name, no abbreviations.
Location	City or other location for the organization.
Common Name	Domain name associated with the certificate.
Subject Alternative Name	Host names and IP addresses protected by this certificate. Click  or  to add or delete a subject.

- 4 Click **GENERATE** to generate the certificate or CSR. Then do one of the following:
 - If you generated a CSR, view it by selecting the View button on the Certificate List screen. Follow the instructions to copy the contents to the clipboard and paste it into a text document to send to the CA.
 - If you generated a self-signed certificate, restart the RealPresence Platform Director server so that it recognizes the certificate.

View, Copy, or Delete a Certificate

From the certificate list, you can view available certificates, confirm if a certificate is required, copy a certificate, or delete an obsolete certificate. This section describes how to view and delete certificates.

To view, copy, or delete a certificate:

- 1 Go to **Admin > Platform Settings**, and then click the **Certificate list** tab to view a list of existing certificates.
- 2 Do one of the following:
 - Click **VIEW** to view and/or download the certificate.

When you view a certificate or CSR, you can also copy the certificate information to upload onto another server or, for a CSR, to send to a CA in order to obtain a signed certificate.

- ◆ Copy the entire hash, from -----BEGIN CERTIFICATE through -----END CERTIFICATE or, for a CSR, -----BEGIN CERTIFICATE REQUEST----- through -----END CERTIFICATE REQUEST-----.
- ◆ Paste the text into a text file.
- ◆ Save the file with a .cer extension for a certificate, or a .csr extension for a CSR.
- Click **DELETE** to delete the certificate.

This option is available only for trust certificates. WebServer certificates and CSRs can be replaced by regenerating (if a CSR or self-signed certificate) or uploaded as a CA-signed certificate. For generating WebServer certificates, see [Generate Certificates and CSRs](#).



Be careful when deleting any trust certificate. Deleting a certificate from a certificate chain produces an incomplete chain. If a chain is incomplete, any certificate that was signed or issued by the CA in that chain will no longer be trusted by the system.

Upload a Certificate or Certificate Chain

You can upload either of the following two types of certificates:

- Third-party certificates signed by a CA that identify the RealPresence Platform Director server.
- Trust certificates.



Upload certificates using either a Chrome or Firefox browser. Internet Explorer is not supported for certificate uploads.

To upload a certificate:

- 1 Go to **Admin > Platform Settings**, and then click the **Upload Certificate** tab to select the settings for the certificate you want to upload.
- 2 Do one of the following to begin uploading the certificate.
 - For a third-party, signed certificate that identifies the RealPresence Platform Director server, from the **Type** list, select **WebServer Own**.
 - For a trust certificate, from the **Type** list, select **WebServer Trust**.
- 3 Browse to the certificate, and click **Open**. Then click **UPLOAD**.

After a certificate is uploaded, the server restarts so that the new certificate will be recognized by the system.

Configure Certificate Settings

- On the Certificate Settings tab, you can control two security-related settings that affect the system's connection with a provider (vCenter). If your RealPresence Platform Director system is not in a vCenter and thus doesn't connect to a provider, these settings have no effect.
- By default, the RealPresence Platform Director system enforces RSA key length for certificates as this provides greater security.

- By default, the RealPresence Platform Director system connects to providers that you add without checking their security certificates.



Do not turn off Ignore Certificates unless all providers (vCenters) in your environment can present valid certificates.

To configure certificate settings:

- 1 Go to **Admin > Platform Settings > Certificate**, and then click the **Certificate Settings** tab.
- 2 To accept provider certificates with short RSA keys (less secure), clear the **Enforce RSA Key Length** check box.
- 3 To check the certificates of all providers (vCenters), clear the **Ignore Certificate** check box.
- 4 Click **UPDATE**.

The server restarts with the new settings.

View and Manage Logs

The RealPresence Platform Director log levels are listed hierarchically in order of greatest to least detail. When you select a log level, the RealPresence Platform Director system begins writing log messages for the selected level, along with all the lower levels. When you want to view logs, you can download the log files.



In a production environment, we recommend setting logging to Informational or below. Set logging to more detailed levels when you're troubleshooting an issue, and then return the setting to Informational or below for day-to-day operations.

To select a log level or download the log file:

- 1 Go to **Admin > Platform Settings**. Then click the **LOGS** tab to display log options.
- 2 Specify the parameters in the table below.

Field	Value/Description
Level	Choose the level in the drop-down list. <ul style="list-style-type: none"> • None Turn off logging. • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Rotation Size	Configures the maximum size the log file can reach before it is rolled.

Field	Value/Description
Rolling Frequency	Configures how often the log file is rolled. When a log file is rolled, a new log file is started and the previous log file is archived on the local server.
Configured File Count	Configures the maximum number of this type of log file that can be stored on the local server.

- 3 Select one of the following options:
 - Click **UPDATE** to begin generating logs at the selected level.
 - Click **DOWNLOAD** to download a *.zip file containing current system logs.

Configure RealPresence Platform Director to use SMTP

You can configure RealPresence Platform Director to use Simple Mail Transfer Protocol (SMTP) to send emails notifying system administrators when alarms are triggered and thresholds reached within the system. RealPresence Platform Director also sends a User Created Notification email to newly added users so that they can access the system and update their credentials.

To configure SMTP settings:

- 1 Go to **Admin > Platform Settings**. Then click the **SMTP** tab.
- 2 Enter SMTP settings as shown in the following table.

Field	Value/Description
Server	Enter the host name or IP address of the email server that will send messages for the RealPresence Platform Director system.
Secure	Select the check box if the SMTP server requires authentication to send messages. Then add a Login ID and Password for that email user.
Port	Enter the port used by SMTP (25 is the default for unsecure email, and 465 is the default for secure email).
Sender Email ID	If Secure is not checked, enter the name of the sender for emails generated from RealPresence Platform Director.
Login ID	If Secure is checked, enter the user name that RealPresence Platform Director will use to authenticate with the SMTP server.
Password	If Secure is checked, enter the password for the user specified in the Login Id field.
Send Email	Select the check box to send a test email from the selected email user.

- 3 Click **UPDATE** to save the SMTP settings. Note that previous settings cannot be reset after they have been updated.

Enable an SNMP Agent on the RealPresence Platform Director System

The following procedure configures an SNMP agent on the RealPresence Platform Director system to allow monitoring of the system itself, using a third-party SNMP manager such as Nagios.



Note: SNMP monitoring of component instances is configured elsewhere.

This configuration is for monitoring of the RealPresence Platform Director system itself.

To enable it to monitor the RealPresence Platform component instances that it manages, enable SNMP in those components and then configure the RealPresence Platform Director system to receive SNMP notifications from each component instance. This is done on each Instance page. See [Enable SNMP for an Instance](#).

To enable SNMP monitoring of the RealPresence Platform Director system:

- 1 Go to **Application Settings > SNMP**.
- 2 Select the **Enable SNMP** check box to enable an SNMP agent on the RealPresence Platform Director system. Then complete the SNMP configuration settings, as shown in the following table. The configuration selections vary depending on which SNMP version you choose.

Fields	Value/Description
SNMP version	The version of SNMP used for this agent (v2c or v3).
Transport	The transport protocol for SNMP communications to the host receiver. RealPresence Platform Director supports only UDP. 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	Port 161, the port on which the SNMP agent communicates. This is 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 should be changed to make the SNMP information more secure.
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.
Location	Specifies the value to be returned for a standard MIB query to identify the geographical or logical location of the server.
Security User	For SNMPv3 only. Specifies the security name required to access a monitored MIB object.

Fields	Value/Description
Authentication type	<p>Specifies the authentication protocol. These protocols are used to create unique fixed-sized message digests of a variable-length message.</p> <p>Possible values for authentication protocol are:</p> <ul style="list-style-type: none"> • MD5—Creates a digest of 128 bits (16 bytes). • SHA—Creates a digest of 160 bits (20 bytes). <p>Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.</p>
Authentication password	<p>For SNMPv3 only.</p> <p>Specifies the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest.</p>
Encryption type	<p>For SNMPv3 only.</p> <p>Specifies the privacy protocol for the connection between the RealPresence Platform Director system and the SNMP manager.</p> <p>The RealPresence Platform Director system implements communication with authentication and privacy (the authPriv security level as defined in the USM MIB).</p> <p>Possible values for privacy protocol are:</p> <ul style="list-style-type: none"> • DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet.
Encryption password	<p>For SNMPv3 only.</p> <p>Specifies the password to be associated with privacy protocol.</p>

- 3 Click **UPDATE** to save the SNMP agent's configuration settings.

Upgrade the RealPresence Platform Director System

You can upgrade RealPresence Platform Director from version 2.0 to the current version using this feature.



Before upgrade to 3.0, you must migrate a version 1.8.x instance of RealPresence Platform Director to a version 2.0 instance; this enables you to import all configuration data (except for NTP settings and certificates) from the old instance. Refer to the RealPresence Platform Director version 2.0 Release Notes on how to do the migration.

To upgrade the RealPresence Platform Director software:

- 1 Download the binary (*.bin) upgrade file from [Polycom Support](#).
- 2 In RealPresence Platform Director, go to **Admin > Platform Settings** and click **UPGRADE**.
The **Upgrade** page displays the current system version and the previous upgrade history, if any. If an upgrade file has already been uploaded but not installed, it's listed under **Upgrade Package Details**.
- 3 Click **Browse**, select the *.bin upgrade file you downloaded, and click **Open**.
- 4 Verify that the file name displayed is correct and click **UPLOAD**.
The system displays the uploading progress. Depending on the size of the upgrade file and network speed, it may take a few minutes.

- 5 After the file has finished uploading, click **UPGRADE**. In the **Confirm** dialog box, click **Yes**.
The system displays an upgrading message, and the interface becomes unavailable. The reboot and upgrade process may take some time, depending on the size of the upgrade. When the upgrade is finished, you're returned to the login page.
- 6 Log back into the RealPresence Platform Director system as a user with Super Admin privileges and accept the End User License Agreement.
- 7 Go to **Admin > Platform Settings** and click **UPGRADE**.
- 8 Verify that System Information now shows the new, upgraded system version and that Upgrade History shows that the upgrade operation was a success.

If you haven't already done so, read the release notes for the version to which you upgraded for information about changes included in the upgrade.

Appendix 1: Network Port Requirements

Network access to and from the RealPresence Platform Director system is achieved through the network ports listed in the following table.

Required network ports

Source IP	Trans-port	Protocol	Source Port	Dest. IP / Port	Note
INBOUND (to REALPRESENCE PLATFORM DIRECTOR)					
<DMA Virtual IP> <RealPresence Access Director Mgmt IP> <RMX-Control & Shelf> <RealPresence Resource Manager Address> <WSP Interface>	TCP	Proprietary	32768-61000	RealPresence Platform Director 3333, 9333	License-related communications between each product instance and RealPresence Platform Director. Frequency of communication from each product to RealPresence Platform Director is at the discretion of each product.
Mgmt PC IP	TCP	(HTTP)/HTTPS	Unknown, depends on Mgmt PC OS	RealPresence Platform Director (80) /443	Mgmt via WebUI (port 80 is not required, but if accessed, it is immediately redirected to 443)
Mgmt PC IP	TCP	SSH	Unknown, depends on Mgmt PC OS	RealPresence Platform Director 22	Mgmt via SSH
DHCP Server	UDP	DHCP	67	RealPresence Platform Director 68	For DHCP responses when DHCP is enabled
SNMP monitoring IP	TCP and/or UDP	SNMPv2, SNMPv3	Unknown, depends on Mgmt PC OS	RealPresence Platform Director 161	SNMP monitoring could be TCP or UDP or both; depends on your NMS

Required network ports

Source IP	Transport	Protocol	Source Port	Dest. IP / Port	Note
<DMA Virtual IP> <RealPresence Access Director Mgmt IP> <RMX-Control & Shelf> <RealPresence Resource Manager> <WSP Interface>	UDP	SNMPv2, SNMPv3	161	RealPresence Platform Director 65001	RealPresence component response to SNMP query originated by RealPresence Platform Director (see outbound 65001 below)
OUTBOUND (from REALPRESENCE PLATFORM DIRECTOR)					
RealPresence Platform Director	TCP	Proprietary	32768-61000	Internet/ Flexera 64.14.29.0/24 (normal) 64.27.162.0/24 (disaster recovery) 443	Licenses for Polycom RealPresence Platform system components managed in online mode
RealPresence Platform Director	TCP	HTTPS	32768-61000	<DMA Virtual IP> <RealPresence Access Director Mgmt IP> <RMX-Control & Shelf> <RealPresence Resource Manager Address> <WSP Interface> 443, 8443	Polycom API communications from RealPresence Platform Director to product instances
RealPresence Platform Director	TCP	HTTPS	32768-61000	VMware vCenter(s) 443	VMware API communications to vCenter(s)
RealPresence Platform Director	TCP	SMTP	32768-61000	The SMTP server configured using the RealPresence Platform Director UI 25	Mail notifications from RealPresence Platform Director The destination port is the SMTP port specified in the RealPresence Platform Director UI

Required network ports

Source IP	Trans-port	Protocol	Source Port	Dest. IP / Port	Note
RealPresence Platform Director	UDP	DHCP	68	DHCP Server 67	DHCP requests to server when DHCP is enabled
RealPresence Platform Director, NTP server(s)	UDP	NTP	123	NTP server(s), RealPresence Platform Director 123	NTP communication is bi-directional over port 123
RealPresence Platform Director	UDP Only	SNMPv2, SNMPv3	65001	<DMA Virtual IP> <RealPresence Access Director Mgmt IP> <RMX-Control & Shelf> <RealPresence Resource Manager Address> <WSP Interface> 161	RealPresence Platform Director's monitoring of each product instance over SNMP (each instance may have its own configuration) The destination port is the SMTP port on each monitored instance

Appendix 2: Troubleshooting

Troubleshooting common system software issues can lessen extended system down times. This section contains general troubleshooting information to help resolve any problems that you might encounter during the setup, configuration, deployment, or management of the RealPresence Platform Director system. The tables in this section list various trouble symptoms, the likely causes of these problems, and recommended corrective actions to take.

Deployment

Deployment Troubleshooting

Problem	Explanation/Solution
Instances are not being created in vCenter.	Check these values in RealPresence Platform Director: Data Store, Data Center, resource pool, and vCenter username and password with administrator rights.
Datastore or data center is not listed correctly.	Check if the server URL is the IP address of the vCenter server (not vSphere).

Management

Management Troubleshooting

Problem	Explanation/Solution
Monitoring: Data does not display for an instance even after several minutes.	Verify that SNMP is enabled for that instance.
Not able to download logs in Internet Explorer.	<ol style="list-style-type: none"> 1. Start the Registry Editor. 2. For a 'per user' setting, locate the following registry key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings For a 'per computer' setting, locate the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings 3. From the Edit menu, click Add Value and add the following value: "BypassSSLNoCacheCheck"=Dword:00000001 4. Exit the Registry Editor.
System Reachability Alarms for a Provider indicate a login failure. Instance last error that indicates too many consecutive login failures. Logs show exceptions with errors indicating too many login failures.	<p>There are several reasons why these errors may happen, but they all have the same solution. Some typical causes include:</p> <ul style="list-style-type: none"> • Credentials for the user connecting to vCenter have changed but have not been updated in RealPresence Platform Director. • Extended network failures when RealPresence Platform Director attempts to connect to the vCenter. <p>Correct the issue by editing the settings for the provider, either entering the correct credentials or updating with no changes. This will reset the failed login attempts and should correct all of the alarm conditions.</p>
After reboot, persistent "still booting" message in web interface.	<p>Clear the cache of your browser, wait a few minutes, and try again. Be sure you're using Chrome or Firefox, not Internet Explorer.</p> <p>Try logging into the secure shell.</p> <p>Try pinging the instance. If it responds, wait for the reboot to complete.</p> <p>If the problem persists for a very long time, use your vSphere or Hyper-V tools to reboot the VM.</p>