Polycom

Military Unique Deployment Guide

7.3 | January 2014 | 3725-72113-001A1

Polycom® RealPresence® Resource Manager System Deployment Guide For Maximum Security Environments

Trademark Information

POLYCOM® and the names and marks associated with Polycom's 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 the property of their respective owners.

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

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.

End User License Agreement

Use of this software constitutes acceptance of the terms and conditions of the Polycom RealPresence Resource Manager system end-user license agreement (EULA).

The EULA for this product is available on the Polycom Support page for the product.

Support Information

For support on your Polycom systems, contact Polycom Global Services at 1-888-248-4143 or go to the Polycom Support Contact page (http://support.polycom.com/PolycomService/support/us/support/Contact_Us.html).

Documentation Feedback

Polycom appreciates your help as we work to improve its product documentation. Send your comments to videoinformationdesign@polycom.com.

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

Contents

About This Guide

This guide provides the first time setup information you need to configure a Polycom® RealPresence® Resource Manager system. Once you've completed first time setup, see Chapter 2 of the *Polycom RealPresence Resource Manager System Operations Guide* for additional configuration and customization tasks you can perform.

The Polycom RealPresence UC solution, when deployed according to the guidancein this document (and those referenced by it) meets the U.S. Department of Defense security and interoperability requirements for listing on the US Department of Defense (DoD) Unified Capabilities (UC) Approve Products List (APL) as maintained by the Defense Information Systems Agency (DISA) Unified Capabilities Connection Office (UCCO).

For more information about the UC APL process please visit the UCCO website.

Documentation Resources

In addition to this guide, the available documentation that describes the RealPresence Resource Manager system includes:

- *Polycom RealPresence Resource Manager System Release Notes*

  Provides the information users need to know about the specific release of the system you're implementing.

- *Polycom RealPresence Resource Manager System Operations Guide*

  Provides more detailed and specialized configuration, operation, and administration information users needs to know when using the RealPresence Resource Manager system.

- *Polycom RealPresence Resource Manager System Web Scheduling Guide*

  Gives schedulers detailed information on scheduling and monitoring conferences.

Assumptions

This guide is written for a technical audience. You will be configuring system networking, and certificates as well as integrating with a time server, and directory server.

This guide assumes that you are starting with a RealPresence Resource Manager system that has never been previously configured.

Document Change History

This information is required for listing on the US Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL):

Doc Version	Release Date	Description
1.0	January 2014	Initial approved release.

To request information or submit comments about this document, please contact Polycom Global Services.

Polycom® RealPresence® Resource Manager System Server Setup

The sections that follow describe the steps required to perform the initial installation and setup of a Polycom® RealPresence® Resource Manager system including:

Conditions of Fielding

The following information is required for listing on the US Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL).

When the system is deployed into an operational environment, the following security measures (at a minimum) must be implemented to ensure an acceptable level of risk for the sites' Designated Approving Authority:

a The system must be incorporated in the site's PKI. If PKI is not incorporated, the following findings will be included in the site's architecture:

- APP3280 for RPRM Rel. 7.3.0J
- APP3290 for RPRM Rel. 7.3.0J
- APP3300 for RPRM Rel. 7.3.0J
- APP3305 for RPRM Rel. 7.3.0J
- APS0110 for RPRM
- DSN13.17 for RPGS; RPRM
- NET0445 for RPGS; RPRM

b The system must be integrated into the site's AD environment for authentication and authorization requirements.

c The site must be a STIG-compliant, Public Key-enabled workstation for management of the solution.

d The configuration must be in compliance with the Polycom RPGS Family Rel. 4.1.0J military-unique features deployment guide.

e The site must register the system in the Systems Networks Approval Process Database <https://snap.dod.mil/index.cfm> as directed by the DSAWG and Program Management Office.

Complete the First Time Setup Worksheet

Before you begin system setup, fill out the **My System Values** column of this worksheet.

Item	My System Values	Factory-Set Default Values	Description
System Network Settings (from Admin > Server Settings > Network)			
System Name		PLCM_RPRM	System name of the RealPresence Resource Manager system. Can be up to 32 characters long; dashes and underscores are valid characters.
DSCP Marker			Allows the administrator to configure the Quality of Service level of the RealPresence Resource Manager. Set the level between 0 - 63.
IPv6 Address			IPv6 global address
IPv6 Prefix length			Within IPv6 networks, the prefix length is the equivilant of the subnet mask in IPv4 networks. Should be 1-128.
IPv6 Default Gateway			The IPv6 address of the gateway server/router. For IPv6 networks only.
IPV6 Link Local Address			Read-only field. The RealPresence Resource Manager system generates a value for this field when IPv6 is enabled.
IPv4 Address		192.168.1.254	Static, physical IP address for the system server on an IPv4 network. 192.168.1.254 is the default value that needs to be changed according to your own network.
IPv4 Subnet Mask		255.255.255.0	Network subnet mask of the system server. For IPv4 networks only.

Item	My System Values	Factory-Set Default Values	Description
IPv4 Default Gateway		192.168.1.1	IP address of the gateway server/router. For IPv4 networks only. 192.168.1.1 is the default value. You need to change this to match the gateway IP for your network.
DNS Domain			This is the DNS domain name suffix for the network in which the domain name server and the system server reside. For example `polycom.com`, not the fully qualified path of <*hostname*>`.polycom.com`.
Preferred DNS Server			IP address of the domain name server.
Alternate DNS Server			IP address of an alternate domain name server. The alternate IP address can does not have to match the network type of the preferred server. For example, the preferred DNS server can be IPv4, while the alternate DNS server can be IPv6.
Enable 802.1.x		Disabled	Enable 802.1.x if your network requires this type of authentication. 802.1.x is commonly required in maximum security environments.
User Name			The user name for the 802.1.x account.
Password			The password for the 802.1.x account
Confirm Password			Confirm the password for the 802.1 x account.
Key Management Protocol			Select the appropriate Key Management Protocol for your environment. When maximum security mode is enabled, this value is hardcoded to be IEEE8021X.
EAP Method			Select the appropriate EAP Method for your environment. When maximum security mode is enabled, only TLS and PEAP are allowed.
Phase2 Protocol			Select the appropriate Phase2 Protocol for your environment.

Item	My System Values	Factory-Set Default Values	Description
System Time Information (from Admin > Server Settings > System Time)			
System Time Zone			
Current Date			
Current Time			
External NTP Server			IP address of external NTP time server (optional).
Information Required for Polycom Customer Support (from Admin > Server Settings > Licenses)			
Serial number			
License number			

Set up DNS Host and Service Records

Before installing a RealPresence Resource Manager system, you should consider configuring your DNS servers to:

- Resolve queries for the RealPresence Resource Manager system by host name.
- Resolve reverse lookup queries for the RealPresence Resource Manager system
- Identify the RealPresence Resource Manager system as a service on the network.

The first function requires a DNS host record and optionally a reverse lookup pointer record. The second function requires a DNS service record.

The DNS should also have entries for your Active Directory server, mail server, and H.323 gatekeepers (if H.323 is deployed).

DNS Host Record

To allow your DNS servers to resolve queries for the RealPresence Resource Manager system by host name, you must enter a DNS host record in your DNS file. The format of this record depends on the format of your network addressing.

- If you use IPv4 addressing, enter a DNS A record in the required format.
- If you use IPv6 addressing, enter a DNS AAAA record in the required format.

To allow your DNS servers to resolve queries for the Resource Manager system by reverse lookup, you must enter a DNS pointer (PTR) record in your DNS file.

Request Certificates

If you are using certificates, you should use the same certificates that you used for the initial installation of the system. If that information is not available, use the information below to set them up.

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

By default, to support encrypted communications and establish a minimal level of trust, the system includes a default key and self-signed certificate. However, to implement a full certificate chain to a root certificate authority (CA), the system requires a root CA certificate, an identity server certificate signed by the root signing CA and a Sub CA certificate. Therefore, at some time you must request these certificates from your CA.

You must install the root CA and intermediate certificates during first time setup, therefore we recommend you obtain them from your CA before beginning first time setup. However, with regard to the identity server certificate you have two options:

- The RealPresence Resource Manager system First Time Setup Wizard supports the function of creating a certificate signing request (CSR). Therefore, you may choose to create the CSR for the identity server certificate during first time setup and suspend the process while you wait for your CA to provide the certificate.
- You can also request the identity server certificate in advance of first time setup, but to do this you must have extensive knowledge of certificates, certificate templates, and CSR structures.

Pre-stage a Computer Account

To enable the **Use Single Signon** option, which allows endpoint users who are included in the Active Directory to securely log into their dynamically- managed endpoints without typing in credentials, an Active Directory administrator must first pre-stage an Active Directory computer account for the RealPresence Resource Manager system.

This procedure can be done at any time before running first time setup.

To pre-stage a computer account

1. On the Active Directory system, use the Microsoft **Active Directory Users and Computers** MMC snap-in to create a computer account for the RealPresence Resource Manager system. Create the computer account in any desired organizational unit (OU). The computer account object must have **Reset Password** and **Write Account Restrictions** permissions.

   For more information on the **Active Directory Users and Computers** MMC snap-in, see Microsoft Technet.

2. From a command window on the Domain Controller, type:

   `net user <computer account name>$ <Password> /domain`

   Where <***computer account name***> is the name of the computer account created in step 1 on page -8, <***Password***> is the desired password, and **/domain** is literally **/domain** (i.e., do not substitute with a domain name). For more information on the `net user` command, see the Microsoft Knowledge Base.

   You have now created a computer account that you can use for integrated Windows authentication.

Prepare Client Systems

To log into the RealPresence Resource Manager system, you need a client system with the following applications.

- Microsoft Internet Explorer® 8.0, 9.0, 10.0
- Adobe® Flash® Player 11.0.x.

If you will be working in a closed network environment, make sure these applications are installed on the client system before beginning First Time Setup.

The RealPresence Resource Manager system's management interface requires Adobe Flash Player. For stability and security reasons, we recommend always using the latest version of Flash Player.

Even so, be aware that your browser's Flash plugin may hang or crash from time to time. Your browser should alert you when this happens and enable you to reload the plugin. In some cases, you may need to close and restart your browser.

Connect to the RealPresence Resource Manager System Server

You configure the RealPresence Resource Manager system server through a ethernet port.

To connect to the RealPresence Resource Manager system

1. Open a browser and enter the static IP address in the address bar.

   `https://<staticipaddress>:8443/flex`

Managing Security Certificates

Certificates are a security technology that assists networked computers in determining whether to trust each other. Each digital certificate is identified by its public key. The collection of all public keys used in an enterprise to determine trust is known as a Public Key Infrastructure (PKI).

To manage digital certificates, an enterprise must:

- Establish a Public Key Infrastructure using one or more Certificate Authorities (CA). Typically, an enterprise's IT department has a CA but commercial CAs may be used as well.
- Configure each computer that participates in the PKI with a digital certificate that identifies it. The certificate must be signed by one of the CAs in the PKI.
- Configure each computer that participates in the PKI to trust the PKI's Certificate Authorities.
- Ensure that the PKI is used to protect data exchange by configuring each system to use encryption protocols such as Secure Sockets Layer (SSL) and/or Transport Level Security (TLS).

This chapter describes the Polycom® RealPresence® Resource Manager system certificate management tasks. It includes these topics:

Configuring RealPresence Resource Manager to Use Certificates

Before installing any certificates or configuring an Online Certificate Status Protocol (OCSP) responder settings, you must configure how the RealPresence Resource Manager system will use certificates.

These settings specify, for example, whether the RealPresence Resource Manager system is allowed to have a self-signed certificate and the validation options that should be applied to certificates from other systems.

You cannot use self-signed certificates if the RealPresence Resource Manager is running in maximum security mode.

When in maximum security mode, you must install certificates during first-time set up.

For more information about maximum security mode, see the *Polycom RealPresence Resource Manager System Deployment Guide for Maximum Security Systems*.

Certificate settings also specify if client systems (endpoints and users who access the RealPresence Resource Manager system user interface) require to present certificates for authentication. Determine the degree in which you want to use certificates within your deployment and configure the settings appropriately.

1. Configure certificate settings.
2. Install certificates on the RealPresence Resource Manager system.
3. Configure OCSP settings.

Configuring Certificate Settings

You can configure how the RealPresence Resource Manager deals with security certificates. How you set up your certificate settings determines the level of security you have for your system.

Some certificate settings are not configurable when your system is in maximum security mode. For more information about maximum security mode, see the *Polycom RealPresence Resource Manager System Deployment Guide for Maximum Security Systems*.

For example, you can require all clients attempting to access the system to present a certificate. You can also allow the system to trust self-signed certificates. The latter example represents a less secure configurations and is not allowed in maximum security environments.

Using Self-Signed Certificates

If you install a full PKI chain after you configured the system to trust self-signed certificates, you should delete the self-signed certificates of any system on which the self-signed certificate has been replaced with a CA signed certificate.

To configure certificate settings

1. Go to **Admin > Management and Security > Certificate Management**.
2. Click **Certificate Settings**.
3. For **Server Settings**, use the following table as guidance:

Table -1 *RealPresence Resource Manager Server Settings*

Field	Description
Cipher Mode	You can choose from the following cipher modes: Standard Ciphers Weak Ciphers Strong Ciphers (FIPS)
Allow self-signed certificate	You can choose to allow a self-signed certificate on the RealPresence Resource Manager system.
Require client to send certificate	This setting requires all clients (endpoints, peripherals, and users accessing the RealPresence Resource Manager system web interface over an encrypted protocol such as SSL or TLS) to send identity certificates in order to access the system.

4. For **External Client Certificate Settings**, use the following guidance:

Field	Description
Trust self-signed certificate	You can choose to trust self-signed certificates from client systems (endpoints, users accessing the web interface, and peripherals). Use this setting with discretion. Any and all self-signed certificates presented by clients will automatically be installed as trusted peer certificates and will be trusted until they are deleted from RealPresence Resource Manager's trusted certificates list. This setting is intended to be used selectively, for example, during initial deployment of a Polycom solution that will use self-signed certificates going forward. After RealPresence Resource Manager has been running for several hours (or days) and all of the known clients' certificates have been added to the RealPresence Resource Manager's trusted certificates list, the setting should be disabled to prevent network intrusion from unknown clients. Disabling the setting does not mean that self-signed certificates will no longer be trusted. It means that no new self-signed certificates will be automatically added to the RealPresence Resource Manager's trusted certificate list.
Validate date range	Choose if you want to validate the date range. When this is checked, the RealPresence Resource Manager verifies the date range contained in the certificate to ensure validity.
Validate revocation	When this is checked, the RealPresence Resource manager validates the revocation status using the revocation resources (OCSP responder URL or CRL Distribution Point).

5 For **External Server Certificate Settings**, use the following guidance:

Field	Description
Trust self-signed certificate	You can choose to trust self-signed certificates from server systems (DMA systems, MCUS and session border controllers). Use this setting with discretion. Any and all self-signed certificates presented by servers will automatically be installed as trusted peer certificates and will be trusted until they are deleted from RealPresence Resource Manager's trusted certificates list. This setting is intended to be used selectively, for example, during initial deployment of a Polycom solution that will use self-signed certificates going forward. After RealPresence Resource Manager has been running for several hours (or days) and all of the known servers' certificates have been added to the RealPresence Resource Manager's trusted certificates list, the setting should be disabled to prevent network intrusion from unknown servers. Disabling the setting does not mean that self-signed certificates will no longer be trusted. It means that no new self-signed certificates will be automatically added to the RealPresence Resource Manager's trusted certificate list.
Validate hostname	When this is checked, the RealPresence Resource Manager verifies the hostname contained in the certificate to ensure validity.
Validate date range	Choose if you want to validate the date range. When this is checked, the RealPresence Resource Manager verifies the date range contained in the certificate to ensure validity.
Validate revocation	When this is checked, the RealPresence Resource manager validates the revocation status using When this is checked, the RealPresence Resource manager validates the revocation status using the revocation resources (OCSP responder URL or CRL Distribution Point).

6 Click OK.

The next step is to install the required certificates on the RealPresence Resource Manager system.

Installing Certificates

This section includes the following topics:

Accepted Certificates

To support encrypted communications and establish a minimum level of trust, the RealPresence Resource Manager system presents a self-signed digital certificate to its clients. This default certificate will typically not be trusted by clients. Web browsers that connect to the RealPresence Resource Manager system user interface will display a warning regarding the certificate.

Participation in a Public Key Infrastructure requires a RealPresence Resource Manager system to have been configured with at least one root CA certificate, and a digital certificate signed by the CA that identifies the RealPresence Resource Manager system.

Certificates come in several forms (encoding and protocol). The following table shows the forms that can be installed in the RealPresence Resource Manager system.

Encoding	Standard / File Type	Description and Installation Method
PEM (Base64-encoded ASCII text)	PKCS #7 standard P7B file	Certificate chain containing: • A signed certificate for the system. • The CA's public certificate. • Sometimes intermediate CA certificates. Upload file or paste into text box.
	CER (single X.509 certificate)	Signed certificate for the system. Upload file or paste into text box.
	Certificate text (can be PKCS#7(P7B) or a single X.509 certificate)	Encoded certificate text copied from CA's E-mail or secure web page. Paste into text box.

Encoding	Standard / File Type	Description and Installation Method
DER (binary format using ASN.1 Abstract Syntax Notation)	PKCS #12 standard PFX file	Certificate chain containing: • A signed certificate for the system. • A private key for the system. • The CA's public certificate. • Sometimes intermediate CA certificates. Upload file. **NOTE** This format does not require a Certificate Signing Request to have been generated by the RealPresence Resource Manager system. PKCS #12 is not supported when the RealPresence Resource Manager system is in maximum security mode or when Strong Ciphers (FIPS) mode is being used.
	PKCS #7 standard P7B file	Certificate chain containing: • A signed certificate for the system. • The CA's public certificate. • Sometimes intermediate certificates. Upload file.
	CER (single certificate) file (X.509 standard format)	Digital certificate that uniquely identifies the system within the PKI. Upload file. **Note** The certificate must have issued by a CA using the most recent Certificate Signing Request generated by the RealPresence Resource Manager system.

Create a Certificate Signing Request

Although the initial RealPresence Resource Manager system configuration permits using the default, self-signed certificate, normal operation in a secure mode requires that you install a digital certificate signed by a trusted certificate authority that uniquely identifies the RealPresence Resource Manager system within your public key infrastructure. This can be done by creating a certificate signing request for the RealPresence Resource Manager system and submitting it to a certificate authority to be signed.

Although it is common for a system to be identified by any number of digital certificates, each signed by a different CA, the RealPresence Resource Manager system currently only supports a single identity certificate.

This procedure describes how to create a certificate signing request (CSR) to submit to a certificate authority.

To create a certificate signing request

1. Go to **Admin > Management and Security > Certificate Management**.

   The **Certificate Management** page displays the list of currently available certificates. By default, the system will have one server certificate identified as the **Resource Manager self-signed certificate** and one or more root certificates or certificate chains.

2. Click **Create Certificate Signing Request**.

   If you see the warning "This action will overwrite any previously generated or uploaded private key. Do you want to continue?," do one of the following:

   - If you are waiting for a previous request to be signed, click **No**. Because the RealPresence Resource Manager system currently supports only one identity certificate, only the most recent private key is retained. The digital certificate resulting from the most recent CSR is the only certificate that will match the retained private key and is therefore the only identity certificate that can be installed.
   - If this is a new certificate signing request, click **Yes** to continue.

3. In the **Certificate Information** dialog box, enter the identifying information for your RealPresence Resource Manager system and click **OK**.

Field	Description
Signature Algorithm	You can select either SHA256 or SHA1. Maximum security mode requires SHA256.
Country Name	Two-letter (ASCII only) ISO 3166 country code in which the server is located.
State or Province Name	Full state or province name (ASCII only) in which the server is located.
Locality Name	City name (ASCII only) in which the server is located.
Organization Name	Enterprise name (ASCII only) at which the server is located.

Field	Description
Organizational Unit Name	Subdivision (ASCII only) of the enterprise at which the server is located. Optional. Multiple values are permitted, one per line.
Common Name (CN)	The host name of the system (read-only), as defined in the network settings.
IPv4 Address	The IPv4 address of the system (read-only), as defined in the network settings.
IPv6 Address	When applicable, the IPv6 address (read-only) of the system, as defined in the network settings.
Email Address	E-mail address (ASCII only) for a contact at the enterprise.

A **File Download** dialog box appears.

4. In the **File Download** dialog box, click **Save**.
5. In the **Save As** dialog box, enter a unique name for the file, browse to the location to which to save the file, and click **Save**.
6. Submit the file (or text within the file) as required by your certificate authority.

   When your certificate authority has processed your request, it sends you a signed digital certificate for your RealPresence Resource Manager system. Some certificate authorities send only the signed digital certificate while others send all of the certificates that form the chain of trust (including intermediate and/or root CA certificates). These certificates may arrive as e-mail text, e-mail attachments, or be available on a secure web page.

Install a Certificate

This procedure describes how to install a certificate or certificate chain provided by a certificate authority. It assumes that you've received the certificate or certificate chain in one of the formats accepted by the RealPresence Resource Manager system. See "Accepted Certificates" on page 16.

Installing certificates requires a system restart and terminates all active conferences.

When you install a certificate, the change is made to the certificate store immediately, but the system will not recognize or use the new certificate until it restarts and reads the changed certificate store.

To install a signed certificate that identifies the RealPresence Resource Manager system

1 Go to **Admin > Management and Security > Certificate Management** and click **Install Certificates**.

A warning appears stating that changes made to the certificates will require a system restart to take effect.

2 In the **Install Certificates** dialog box, do one of the following:

- If you have a PKCS#12, PFX, P7B, or single certificate file, click **Upload certificate**, enter the password (if any) for the file, and browse to the file or enter the path and file name.

  PKCS #12 is not supported when the RealPresence Resource Manager system is in maximum security mode or when Strong Ciphers (FIPS) mode is being used.

- If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box at the bottom of the dialog box. You can paste multiple PEM certificates one after the other.

3 Click **OK**.

If you are uploading a signed identity certificate for the first time, it will replace the RealPresence Resource Manager system self-signed certificate.

4 If you are uploading a signed identity certificate for the first time, you can verify that the new signed certificate has replaced the default self-signed certificate:

a In the list of certificates, select the **Resource Manager certificate** and click **View Certificate Details**.

b When the **Certificate Details** dialog box appears, verify that the information in the **Issued To** and **Issued By** sections matches the hostname of the RealPresence Resource Manager and the certificate from the certificate authority.

c Click **Close** to close the dialog box.

Delete a Certificate

You can delete certificates from the system, but the RealPresence Resource Manager system prevents you from deleting any certificate that breaks the identity certificate's chain of trust. To delete these certificates, new CA certificates must be installed and the identity certificate must be replaced.

Removing certificates requires a system restart, which terminates all active conferences.

When you remove a certificate, the change is made to the certificate store immediately, but the system continues to use the removed certificate until it restarts and reads the changed certificate store.

To delete a certificate

1 **Admin > Management and Security > Certificate Management**.

The **Certificate Management** page displays the list of currently available certificates.

2 Select the certificate to be deleted and click **Delete Certificate**.

A warning appears stating that changes made to the certificates will require a system restart to take effect.

3 Click **Yes** to continue.

4 When prompted, click **Yes** to confirm the deletion.

A dialog box informs you that the certificate has been deleted.

View Certificates and Certificate Details

To view the list of installed certificates

1 Go to **Admin > Management and Security > Certificate Management**.

The **Certificate Management** page displays the list of currently installed certificates. By default, the system will display only one certificate. It will be identified as the **Resource Manager self-signed certificate**. When other certificates are installed, they will display along with the server identity certificate.

The **Certificate Management** page has this information.

Column	Description
Status	The status of the certificate. Possible values include: • Certificate is valid • Certificate is invalid
Alias	The certificate name as assigned by the CA

Column	Description
Common Name	This is most often the fully qualified domain name of the server to which the certificate has been issued. If the certificate identifies a client (trusted peer) it might contain the name of a user or the name of an endpoint.
Purpose	The type of certificate. Possible values are: • RealPresence Resource Manager self-signed—the system identity certificate. • Trusted root certificate—the root certificate for a CA. • Intermediate certificate—certificate from an intermediate CA. • Trusted peer—certificate from any server or computer that is not a CA but whose identity is trusted.
Expiration	The expiration date of the certificate.

2 To view more information about a certificate, select the certificate and click **View Certificate Details**.

The **Certificate Details** dialog box appears with this information.

Section	Description
Certificate Info	Purpose and alias of the certificate.
Issued To	Information about the entity to which the certificate was issued and the certificate serial number.
Issued By	Information about the issuer.
Validity	Issue and expiration dates.
Fingerprints	SHA1 and MD5 fingerprints (checksums) for confirming certificate.
Public Key	The certificate's public key, which in the public key infrastructure is distributed widely, and is not kept secure.

3 Use the arrows to reveal or hide information. Click **Close** when you are done.

View the Expiration Dates for Certificates

Certificates and certificate revocation lists expire. To view their expiration dates, see "Create a Certificate Signing Request" on page 17.

Configuring OCSP Settings

The RealPresence Resource Manager system supports using OCSP to verify the status of a certificate. This is an alternative to manually uploading CRLs (Certificate Revocation Lists). If your network does not include an OCSP responder, the RealPresence Resource Manager system parses individual certificates for a CRL Distribution Point URL. There is no need to upload a CRL to complete your certificate validation.

When configuring the RealPresence Resource Manager system to use an OCSP responder, you can either use the default OCSP information that is included in the certificates you receive or explicitly define the OCSP responder location. You should only define an explicit OCSP responder location if your deployment relies on a global OCSP responder.

To configure an OSCP settings for your certificate(s):

1. Go to **Admin > Management and Security > Certificate Management**.
2. Mark the **Enable OCSP** check box if your organization's PKI includes OCSP responders for revocation checking.
   - If you do not specify an OSCP responder location, the OCSP responder URL presented in client or server certificate will be used for validation.
     - If the certificate being presented contains a CDP (CRL Distribution Point), it will be used to check revocation.
     - If there is no CDP in the certificate, revocation check fails and certificate is not trusted.
   - If OCSP is enabled and NO responder URL has been specified:
     - If the certificate contains an OCSP URL it will be used to check revocation.
     - If the certificate doesn't contain the OCSP URL then if the certificate contains a CDP it will be used to check revocation.
     - If the certificate doesn't contain a CDP revocation check fails and certificate isn't trusted.
   - OCSP is enabled and a global responder URL has been specified the global responder is used to check revocation.
     - If the global responder cannot be contacted then if the certificate contains a CDP it will be used to check revocation.

» If the certificate doesn't contain a CDP revocation check fails and the certificate isn't trusted.

3 Click **Verify OCSP Configuration**.

The RealPresence Resource Manager system verifies that it can reach the OCSP responder.

4 Click **Save OCSP Configuration**.

The RealPresence Resource Manager system saves this configuration.

5 After making any changes, you must reboot the system.

Polycom® RealPresence® Resource Manager System Software Setup

The sections that follow describe the Polycom® RealPresence® Resource Manager system software First Time Setup Wizard.

First Time Setup Wizard

When you log into a RealPresence Resource Manager system that has not been configured, the First Time Setup Wizard automatically steps you through a series of ordered configuration pages. You cannot use the system until you've completed the steps in the first time setup.

Note that changing configuration settings on some pages of the First Time Setup Wizard, such as the **System Information** page, will cause the system to reboot. When you log into a system after one of these reboots, the next page in the ordered configuration pages appears.

Complete the First Time Setup Wizard

The first time setup wizard walks you through setting up the initial configuration of your RealPresence Resource Manager system.

To complete the first-time setup wizard

1. On the computer you connected to the system sever (as described in Connect to the RealPresence Resource Manager System Server on page 9), open a browser window.
2. With First Time Setup Worksheet in hand, enter the static, physical IP address or host name for the RealPresence Resource Manager system in the **Address** field.
3. When the system login screen appears, if necessary select a different **Language**.
4. Enter the administrator **Username** and **Password**.

   The factory default is `admin`/`admin`.
5. Click **Login**.

   Because the system has not previously been configured, the **Licensing** page of the setup wizard appears.

EULA License Agreement

6 Read the end-user license agreement (EULA).

Please note that the EULA includes important definitions and usage limitations that will apply to your installation.

7 To accept the EULA terms and conditions, click **Accept**.

Maximum Security Mode

8 Enable maximum security mode.

9 Select whether you want to use Maximum Security Mode.

This mode is NOT recommended for most configurations. Be sure you need maximum security mode before selecting. Once you select Maximum Security Mode, many features of the RealPresence Resource Manager system are disabled.

Administrator Password

10 When the **Change Administrator Password** page appears, enter the **Old Password.**

11 For the **New Password**, enter a new password with a length of at least ten characters.

12 **Confirm the New Password** and click **Next**.

The **Login Banner** page appears.

Login Banner

13 To create a customized login banner for your business, select **Custom** in the **Message pull-down menu** and enter a new login banner into the **Long Banner** and **Short Banner** field.

14 To use one of the pre-configured banners, choose from one of the four sample banners using the **Message** pull-down menu..

15 Click **Next**.

The **Network** page appears.

Network Settings

16 Enter the **Network Settings** information recorded in Complete the First Time Setup Worksheet on page 5 and click **Next**.

The **System Time** page appears.

System Time

17 Configure these settings on the **System Time** page, as necessary.

Field	Description
System Time Zone	The time zone in which the system server resides.
Use Current Time	Select this checkbox to input the current date and time. Even if you plan on using an NTP server, you should set the proper time during first-time setup to ensure certificate creation works reliably.

Field	Description
Current Date	The system date for the system.
Current Time	The system time for the system.
Use External NTP Server Time Synchronization	(Recommended) Select this check box to synchronize the system date and time with an external NTP server. Do this ONLY after you have first manually set the local system time.
IP address or DNS resolved names separated by spaces	The IP address or fully qualified domain name (ASCII only) of the NTP servers.

If you set the system to use an external NTP server without first setting the current date and time, the system time may be wrong until the system's first synchronization.

18 Click **Next**.

The **Certificates** page appears. By default the system is configured to use a default self-signed certificate. Click **Yes** to confirm.

Certificate Management

19

If you have changed the system name of the RealPresence Resource Manager you can generate a new self-signed certificate at this time.

20 To configure and install certificates, please see Managing Security Certificates on page 11.

Be sure to uncheck the **Require client to send certificate** check box at this time to avoid connection problems that could occur. You can enable this setting after first-time setup.

21 Suspend the First Time Setup Wizard until your certificate authority has processed your request:

a Wait until you receive the signed identity server certificate for your system and the CA's certificate revocation list. You may also received intermediate certificates. Depending on the certificate authority, these files may be communicated as mail text, mail attachments, or on a secure web page.

22 For **OCSP Settings**, leave the **OCSP Responder URL** blank. You will configure it later.

23 In **Certificate Settings** be sure to uncheck **Require client to send certificate**. You can mark this setting after completing the First Time Setup.

24 Click **Next**.

System Reboot

25 When prompted to reboot, click **Secure the System and Reboot**. Do NOT choose **Continue Working**.

The system reboots.

26 Close your browser and wait at least five minutes. Wait for the system to completely reboot.

27 If prompted to select a certificate to present, select the appropriate certificate and click **OK**. You may be asked more than once.

28 Accept the security banner.

29 Login using the newly configured local administrator name and password.

Enterprise Directory Server Configuration

30 To integrate the system with an enterprise Active Directory server so that users can include enterprise groups, users, and rooms in their conferences:

a On the **Enterprise Directory** page, select **Integrate with Enterprise Directory Server**.

b To have the system auto-discover the server by querying DNS, enable **Auto-discover** in the **Enterprise Directory Server DNS Name** section; otherwise, enter the **DNS Name** for the enterprise directory server.

31 As needed, configure these settings.

Setting	Description
Domain\Enterprise Directory User ID	Domain and Enterprise Directory User ID for an account that the RealPresence Resource Manager system can use to access the enterprise directory server and retrieve group, user, and room information. This is the account created Pre-stage a Computer Account on page 8. This User ID must have read permissions so it can search the entire forest on the enterprise directory server. In maximum security environments, this User ID is automatically associated with the RealPresence Resource Manager system No Defined Role.
Enterprise Directory User Password	The password for the enterprise directory user account
Security Level	The level of security on the connection between the RealPresence Resource Manager system and the enterprise directory server. Possible values include: • **StartTLS**—The connection is secured over outbound port 3268 (the same port as **Plain**), but it then negotiates security once the socket is opened. Some LDAP servers reject any unsecured transactions, so the first command is the `StartTLS` negotiation command.
Ignore Disabled Enterprise Directory Users	Check this field to have the RealPresence Resource Manager system ignore disabled enterprise users in its queries.
Enterprise Directory Exclusion Filter	If necessary and you understand the filter syntax, specify other types of user accounts to exclude. Don't edit these expressions unless you understand LDAP filter syntax.
Enterprise Directory Search BaseDN	If necessary and you understand the filter syntax, specify the top level of the enterprise directory tree (referred to as the base DN) to search. Don't edit these expressions unless you understand the filter syntax.

32 To integrate the system with an Active Directory domain controller for single sign-on authentication:

a On the **Enterprise Directory** page, select **Allow Delegated Authentication to Enterprise Directory Server**.

The system can auto-discover the closest logical domain controller and Active Directory servers, but to do this the network DNS server must have a DNS SRV record for these servers.

b If your network DNS server has a DNS SRV record for the domain controller, in the **Domain controller name** section enable **Auto-discover**; otherwise, enter the **Fully Qualified Host Name** of the domain controller (for example, `dc1.mydomain.com`). The pre-staged computer account must be within this domain as well.

c In the **Computer Account Credentials** section, enter the **Domain\Computer Name** and **Password** for the pre-staged computer account created in step Pre-stage a Computer Account on page 8.

This check box does not enable non-LDAP protocols if your system is in a maximum security mode. Non-LDAP protocols are not supported when the system is in maximum security mode.

33 Click **Next**.

The system displays the message that you have completed first time setup. You have the option of logging out of the system or being redirected to the system **Dashboard**.

34 Click **Next** to go to the system **Dashboard**.

Complete the System Configuration

Once you've finished first time setup, you will need to perform additional configuration tasks. These tasks are discussed in Chapter 2 of the *Polycom RealPresence Resource Manager System Operation Guide*. For example:

- For maximum security systems, complete certificate configuration
  - Configure your **Certificate Settings** to **Require client to send certificate**
  - Configure the OCSP Responder URL if needed. The OCSP responder URL is required if a certificate does not have an AIA field or a CDP field. It is also required if you are not using CRL-based revocation checking. Check with your PKI administrator.
- Configure your system for redundancy.
- Add licenses to your system.
- Set up your site topology.
- As needed:
  - Integrate with a DMA system for gatekeeper, and virtual meeting room services.
  - Integrate the system with a Microsoft Active Directory.
  - Configure Areas. (Area functionality is a separately licensed feature.)

- Associate users with roles. You will need at least one user with the device administrator role who will be able to create machine accounts for devices. You will also need at least one user assigned to the role of operator or scheduler/advanced schedule so conferences can be scheduled.
- Add machine accounts for all dynamically managed HDX systems and RealPresence Group systems.
-
- Associate users and rooms with machine accounts.
- Associate machine accounts with endpoints.
- Associate users with endpoints.
- Create provisioning profiles and rules for dynamically managed endpoints.
- Add MCUs.
- Enable a management port Whitelist.

  If required, you can limit access to the RealPresence Resource Manger's web interface and SNMP interface from only a set of known IP addresses.

Working with a Polycom Resource Manager System at Maximum Security Level

This section provides the latest information for security-conscious businesses implementing RealPresence Resource Manager system in maximum security mode. It has the following sections:

- Log Into the RealPresence Resource Manager System
- RealPresence Resource Manager System Site Map
- Roles, Permissions, and Functions
- RealPresence Resource Manager System Functionality
  - Conference Scheduling
  - Endpoint Management
  - Network Device Management
  - User Management
  - Group Management
  - Reporting
  - Device Administration
  - System Administration
  - Troubleshooting

IMPORTANT

When you enable RealPresence Resource Manager for Maximum Security level, (the level required in a strict security networks), you cannot change the security level.

Log Into the RealPresence Resource Manager System

To log into the RealPresence Resource Manager system web interface, you need:

- Microsoft Internet Explorer® 8.0 or 9.0
- Adobe® Flash® Player 11.x
- The IP address or, preferably, host name of the RealPresence Resource Manager system and your user name, password, and domain.
- A certificate installed in your browser that is issued by a CA that is known and trusted by the RealPresence Resource Manager system.

By default, the system gives you three opportunities to enter a correct password. (A user assigned the **Administrator** role can change this option.) After three failed attempts, the system returns an error message.

To log into the system

1. Open a browser window and in the **Address** field enter the Resource Manager system server IP address or fully-qualified domain name (FQDN).
   - If you cannot connect, there are likely certificate issues.
   - If you receive a **Security Alert**, click **Yes**.
   - If prompted to install the Adobe Flash Player, click **OK** and follow the installation instructions. If you have access to the Internet, the preferred method is to install the latest version from Adobe.
2. When the system **Login Banner** appears, read the banner and click **Accept** to accept the terms and continue.
3. When the RealPresence Resource Manager system login screen appears, enter your **Username** and **Password**.
4. If necessary, select a different **Language** or **Domain** and click **Login**.

   Because the RealPresence Resource Manager system is a role-based system, users see only the pages and functions available to their role.

RealPresence Resource Manager System Site Map

The following figure shows the site map for a RealPresence Resource Manager system running in maximum security mode. It illustrates the organization of the system interface and the pages available to each of the pre-defined RealPresence Resource Manager system roles.

ADMINISTRATOR ROLE

- CONFERENCE
  - Direct Conference Templates
  - Conference Settings
- ENDPOINT
  - Monitor View
  - Peripherals View
  - Dynamic Management
    - Provisioning Status
    - Provisioning Rules
    - Provisioning Profiles
    - RPAD Server Provisioning Profiles
    - Bundled Provisioning Profiles
    - E.164 Numbering
    - System Naming
    - SIP URI
    - Software Update Policies
    - Access Control Lists
  - Scheduled Management
    - Provisioning
    - Provisioning Profiles
    - Schedule Software Updates
    - Upload Software Updates
    - Endpoint Management Settings
- NETWORK DEVICE
  - Monitor View
  - VBPs
  - SBCs
  - MCUs
  - DMA
  - RPADs
- NETWORK TOPOLOGY
  - Site Topology
  - Sites
  - Site-Links
  - Site-to-Site Exclusions
  - Network Clouds
  - Territories
- USERS
  - Users
  - Groups
  - User Roles
  - Guestbook
  - Rooms
  - Machine Accounts
- REPORTS
  - Site Statistics
  - Site-Link Statistics
  - Endpoint Usage Report
  - Conference Usage Report
  - Conference Type Report
  - Report Administration
- ADMIN
  - Directories
    - Address Books
    - Global Address Book
    - Enterprise Directory
    - Directory Setup
  - Areas
  - Server Settings
    - Network
    - System Time
    - Licenses
    - Redundant Configuration
    - System Logos
    - E-mail
    - SNMP Settings
- ADMIN (continued)
  - Management and Security
    - Security Options
    - Certificate Management
    - Database Security
    - Session Management
    - Banner Configuration
    - Local User Account Configuration
    - Local Password Requirements
    - Whitelist
  - Alert Settings
    - Resource Manager Alert Level
    - Resource Manager Alert Threshold
    - Endpoint Alert Level Settings
    - Remote Alert Profiles
    - Remote Alert Setup
  - Maintenance
    - Server Software Upgrade
    - Backup System Settings
    - Database
    - Troubleshooting Utilities
    - System Log Files
    - Audit Log Files

DEVICE ADMINISTRATOR ROLE

- ENDPOINT
  - Monitor View
  - Peripherals View
  - Dynamic Management
    - Provisioning Status
    - Software Update Status
  - Scheduled Management
    - Provisioning
    - Schedule Software Updates
    - Endpoint Management Settings
- NETWORK DEVICE
  - Monitor View
  - VBPs

OPERATOR ROLE

- CONFERENCE
  - Future
  - Ongoing
  - Anytime
  - Favorites
- ENDPOINT
  - Monitor View
- NETWORK DEVICE
  - MCUS
- USERS
  - Guestbook
- REPORTS
  - Endpoint Usage Report

SCHEDULER/ADVANCED SCHEDULER ROLE

- CONFERENCE
  - Future
  - Ongoing
  - Anytime
- USERS
  - Guestbook

AUDITOR ROLE

- ADMIN
  - Maintenance
    - System Log Files
    - Audit Log Files

Roles, Permissions, and Functions

The following sections identify the pre-defined roles for a RealPresence Resource Manager system running in maximum security mode and the permissions with which they are associated.

Note

The role names (for example, **Administrator**, **Operator**, and **Scheduler**) are not localized into other languages.

No Predefined Role

This role is only available when running the RealPresence Resource Manager system in maximum security mode. By default, when new local users are added to the system, they are assigned No Predefined Role. By default, when the RealPresence Resource Manager system is integrated to an enterprise directory server, all enterprise users are assigned No Predefined Role.

Users who have No Predefined Role cannot access the system; they have no permissions or functions available to them until they are explicitly assigned a role by a user assigned the Administrator role.

Administrator

When users who are assigned the **Administrator** role log into the RealPresence Resource Manager system, they see the **Endpoint**, **Network Device**, **User**, **Reports,** and **Admin** menus and the system **Dashboard** is displayed. They have access to all system functionality except that associated with auditing the system and scheduling, monitoring, or managing conferences or devices.

Device Administrator

When users who are assigned the **Device Administrator** role log into the RealPresence Resource Manager system, they see the **Endpoint**, **Network Device**, and **Admin** menus and the system **Dashboard** is displayed. They can perform device-related functions including adding, editing, and deleting endpoints, MCUs as well as a DMA system. They can also monitor endpoints as well as perform provisioning and software update operations.

Auditor

When users who are assigned the **Auditor** role log into the RealPresence Resource Manager system, they see the **Reports** menu and the system **Audit Log Files** page is displayed. They can run specific system reports that

document security-related events, such as successful and unsuccessful login attempts, gathered from the system. They can also backup, archive, and then delete audit logs.

Operator

When users who are assigned the **Operator** role log into the RealPresence Resource Manager system, they see the **Conference**, **Endpoint**, **Network Device**, **User**, and **Reports** menus and the **Ongoing** conference page is displayed. They can monitor and manage all ongoing system conferences; monitor all devices; delete entries from the system **Guest Book**; and view some system reports.

Scheduler

When users who are assigned the **Scheduler** role log into the RealPresence Resource Manager system, they see the **Conference** and **User** menus and the **Future** conference page is displayed. They can schedule, monitor, and manage their own conferences. They can also delete entries from the system **Guest Book**. They cannot see conferences that they did not create.

Advanced Scheduler

When users who are assigned the **Advanced Scheduler** role log into the RealPresence Resource Manager system, they see the **Conference** and **User** menus and the **Future** conference page is displayed. They can schedule, monitor, and manage their own conferences. They can also edit some conference settings for their scheduled conferences and delete entries from the system **Guest Book**. They cannot see conferences that they did not create.

View Only Scheduler

When users who are assigned the **View Only Scheduler** role log into the RealPresence Resource Manager system, they see the **Conference** and **User** menus and the **Future** conference page is displayed. They can monitor all ongoing system conferences within the areas to which they are associated.

RealPresence Resource Manager System Functionality

When the RealPresence Resource Manager system is running in maximum security mode, there are many operational differences from a less secure mode.

- Maximum security mode includes support for the following new features:
  - Increased security options
  - Certificate management
  - IPv6
  - Encrypted passwords
  - Standard and customized login banners
  - Secure HTTPs
- When in maximum security mode, the RealPresence Resource Manager system supports the following devices:
  - Polycom RealPresence Group endpoints running operating in dynamic management mode and configured at Maximum Security level.
  - Polycom RMX 1500/2000/4000 conferencing platforms running and configured at Maximum Security level.
  - Polycom RealPresence DMA system running and configured at Maximum Security level.
- Maximum security mode does not include support for the following features:
  - Redundant configurations
  - ISDN scheduling
  - External database
  - Global Address Book
  - Standard (scheduled) management and monitoring of endpoints
  - Presence
  - SSH connections
  - Integration with Microsoft Exchange for calendaring
  - Integration with Microsoft Lync Server or Office Communications Server
  - Polycom CMA Desktop clients
  - Polycom RealPresence Desktop clients
  - Audio only conferences
  - Online Help

The following sections describe in detail the operational differences for a RealPresence Resource Manager system running in maximum security mode.

Conference Scheduling

Conference scheduling functionality is available to users assigned the basic scheduler, advanced scheduler, and operator roles. The conference scheduling workflow for pooled conferences on a RealPresence Resource Manager system running in maximum security mode does not change.

You can only schedule H.323 conferences when in maximum security mode.

However, because all direct conferences must be hosted on RMX conferencing systems, the **MCU Settings** for all **Conference Templates** has changed in the following ways:

- The **Supported MCUs** section lists only **RMX** systems.
- The **Always Use MCU** option on the **Conference Template** page is not available (grayed-out); it is always enabled and cannot be changed.

Endpoint Management

Endpoint management functionality is available to users assigned the device administrator role. Users assigned the standard administrator role may only monitor endpoints.

The endpoint management workflow on a RealPresence Resource Manager system running in maximum security mode only supports RealPresence Group system endpoints operating in dynamic management mode. The system changes made to support this workflow change include:

- The **Scheduled Provisioning** and **Scheduled Software Update** pages and the **ACTIONS** associated with them are not available.
- Only RealPresence Group systems and Polycom HDX endpoints that are automatically provisioned by the RealPresence Resource Manager system are displayed in the endpoint list.
- The **ACTIONS** on the **Endpoint > Monitor View** page changes as follows:

Command	Use this command to...
Add	Not available in maximum security mode. Endpoints can only be added to the system during automatic provisioning.
Send Message	Not available in maximum security mode.
Reboot Device	Not available in maximum security mode.
Search Devices	Not available in maximum security mode.

- The **Device Summary** section of the **Endpoint > Monitor View** page does not change.
- The **Device Status** section of the **Endpoint > Monitor View** page changes as follows:

Field	Description
Gatekeeper Registration	The status of the device's registration with the gatekeeper service.
Directory Registration	The status of the device's registration with the enterprise directory server.
Presence Registration	Not displayed when the system is in maximum security mode.
SIP Registration	Supported for Group system endpoints only. Displays the status of a Group system's registration with the SIP server. For HDX endpoints, the status of the device's registration with the SIP server always indicates **Unknown.**
Device Managed	Value displays **OK** if heartbeat has not timed out.
Gatekeeper Address	The IP address of the gatekeeper to which the device is registered.
Device Local Time	The local time on the device machine.
ISDN Line Status	Supported for HDX endpoints. Displays the status of the ISDN line.
ISDN Assignment Type	How the ISDN type was assigned to the device. This always indicates **Undefined**.
Device ISDN Type	Supported for HDX endpoints only. Displays the status of the ISDN type.

- The **Call Info** section of the **Endpoint > Monitor View** page does not change.
- The **Provisioning Details** section of the **Endpoint > Monitor View** page does not change.

Provisioning a Polycom RealPresence Group System

- When dynamically-provisioning the RealPresence Group system, you need to provision the system with the same hostname that was defined when the RealPresence Group system was first installed.

The hostname provisioned by the RealPresence Resource Manager must match the hostname used for the security certificate for the RealPresence Group system, otherwise, you will need to re-do the certificates on the endpoint to match the new hostname with which it was provisioned.

- In order for the RealPresence Resource Manager in maximum secure mode to be able to provision a RealPresence Group system, the Polycom Group system must be using the Maximum Security Profile and have all appropriate certificates installed. For more information about using a RealPresence Group system in a maximum security environment, please see the *RealPresence Group Series Deployment Guide for Maximum Security Environments*.

Network Device Management

Network device management functionality is available to users assigned the device administrator role. Users assigned the standard administrator role may only monitor network devices.

The network device management workflow on a RealPresence Resource Manager system running in maximum security mode does not support session border controllers. The system changes required for this workflow change include:

- The **VBPs**, **RPAD** and **SBC** pages and the **ACTIONS** associated with them are not available.
- The **ACTIONS** on the **DMA > Monitor View** page do not change.
- The **ACTIONS** on the **MCU > Monitor View** page do not change.
- The **Add New Device** dialog box for the RMX MCU does not change.

User Management

User management functionality is divided among different roles: scheduler, operator, and administrator.

Scheduler

Users assigned the basic scheduler and advanced scheduler role can add guest participants to the **Guest Book**.

The **Guest Book** workflow for schedulers on a RealPresence Resource Manager system running in maximum security mode does not change.

Operator

Users assigned the operator role can add, edit, and delete guest participants from the **Guest Book** as well as add, edit, and delete their own **Favorites** lists.

The **Guest Book** and **Favorites** workflow for operators on a RealPresence Resource Manager system running in maximum security mode has not changed.

Administrator

The administrator's user management functionality and workflow changes significantly when the RealPresence Resource Manager system is running in maximum security mode.

When integrated with an enterprise directory (Microsoft Active Directory), the RealPresence Resource Manager system can have only one local account—the default administrator account used to access and administer the system. This account cannot be deleted under any circumstances.

When integrated with an enterprise directory, this local administrator can perform the following user management functions:

- Integrate the RealPresence Resource Manager system with Active Directory. Note that when you integrate the RealPresence Resource Manager system with an Active Directory, all local users other than the default local administrator are removed from the system.
- Edit a subset of enterprise user attributes, such as their role, area, or endpoint associations. This allows the local administrator to assign the administrator role to enterprise users.
- Troubleshoot and administrate the system if the Active Directory connection to the system is lost.

When not integrated with an enterprise directory, this local administrator can perform the following user management functions:

- Add users.
- Edit local user attributes including their contact information and other user attributes such as their role, area, or endpoint associations.
- Delete local users.

The user management workflow on a RealPresence Resource Manager system running in maximum security mode changes in the following ways:

- Once integrated with an enterprise directory, the local administrator can see enterprise users as well as associate them to endpoints, roles, and areas (when applicable).
- Administrators cannot create custom roles with a custom set of permissions. The system has only pre-defined roles and associated permissions as described in "Roles, Permissions, and Functions" on page 32.

  The system changes required to support this workflow change are:

  - The **User Roles** page and the **ACTIONS** associated with it are not available.

- Administrators can no longer assign users more than one role.

  The system change required to support this workflow change is:
  The user interface for assigning roles (**Add/Edit User > Associated Roles**) has changed to a radio button list from which you can assign only one role from a set of mutually exclusive, predefined options.

Disabled local users (when not integrated with an enterprise directory) still appear in the RealPresence Resource Manager system **Users** list. However, disabled enterprise users (when integrated with an enterprise directory) won't appear in the RealPresence Resource Manager system **User** list if the **Ignore Disabled Enterprise Directory Users** option on the **Enterprise Directory** page is enabled.

- Users can no longer be associated with an alert profile because a RealPresence Resource Manager system running in maximum security mode does not include remote alerts.

  The system change required to support this workflow change is:
  The **Add/Edit User > Associated Alert Profile** tab has been removed from the user interface.

A RealPresence Resource Manager system running in maximum security mode includes new password requirements, local user account configuration requirements, and session management requirements that affect local users and local user accounts. For more information about these requirements, see "Management and Security" on page 45.

Group Management

Group management functionality is available to users assigned the administrator role.

The group management workflow on a RealPresence Resource Manager system running in maximum security mode has not changed except that users can no longer inherit roles from groups.

When not integrated with an enterprise directory, local administrators can add local groups with local users. When integrated with an enterprise directory, the single local administrator and any enterprise users assigned the administrator role can **Add** local groups, **Import Enterprise Groups**, and **Synchronize Groups** with Active Directory.

Reporting

Reporting functionality is divided among different roles: administrator, operator, and auditor.

Administrator

The administrator's reporting functionality and workflow changes when the system is running in maximum security mode. Users assigned the administrator role can access the following system reports:

- Endpoint Usage Report
- Conference Type Report
- System Log Files
- Audit Log Files

Users assigned the administrator role can no longer access the following system reports, since these reports have been removed from the system:

- Site Statistics
- Site-link Statistics
- Conference Usage Report

For more information on these reports, see the *Polycom RealPresence Resource Manager System Operations Guide*.

Operator

The operator's reporting functionality and workflow changes somewhat on a system running in maximum security mode. Users assigned the operator role can only access the following system report:

- Conference Usage Report

Users assigned the operator role can no longer access the following system reports:

- Endpoint Usage Report

For more information on these reports, see the *Polycom RealPresence Resource Manager System Operations Guide*.

Auditor

Users assigned the auditor role can access the following system reports:

- Endpoint Usage Report
- System Log Files
- Audit Log Files

For more information on these reports, see the *Polycom RealPresence Resource Manager System Operations Guide*.

The auditor workflow on a RealPresence Resource Manager system running in maximum security mode allows the auditor to:

- View online the **Endpoint Usage Report** for selected endpoints.

  The system change required to support this workflow change is:
  The **Endpoint Usage Report** menu option and page is available from the **Reports** menu, but the **Generate Report** and **Download All CDRs** options are not available to the auditor.

- Download the **System Log Files**.

  The system changes required to support this workflow change are:

  — The **System Log Files** menu option and page is available from the **Reports** menu.

  — The **Download ALL** command is available from the list of **ACTIONS**.

- **Backup and Delete** audit log files.

  The system changes required to support this workflow change are:

  — The **Audit Log Files** menu option and page is available from the **Reports** menu.

  — The **Backup and Delete** command is available from the list of **ACTIONS**. This option allows an auditor to backup and delete selected audit logs. During this process, the RealPresence Resource Manager system requires that the auditor download and run a verification utility that performs a checksum operation to make certain that the downloaded audit log is complete and uncorrupted before the audit log is deleted from the system.

- Change the audit log **Alert Level**.

  The system change required to support this workflow change is:
  The **Change Settings** command is available from the list of **ACTIONS**. By default the audit log **Alert Level** is set to 70% of the **Max File Size Usage**, which is 2 gigabytes.

Device Administration

Only users assigned the device administrator role can perform device administration tasks.

In addition to the tasks described in the Endpoint Management section, the device administrator workflow on a system running in maximum security mode allows the device administrator to:

- See the system **Dashboard**.
- Add, edit, and delete machine accounts for endpoint systems.

  The system change required to support this workflow change are:

  — The Machine Accounts menu option and page is available from the **Admin > Management and Security** menu. Before the RealPresence Resource Manager system can dynamically manage a HDX system or a RealPresence Group system, a user with the device administrator

role must add a machine account for the system. This is the same username that the endpoint's system administrator should enter on the system for the provisioning service. This allows the Polycom endpoint and RealPresence Resource Manager system to authenticate and communicate without using a specific user's account.

About Machine Accounts

Before the RealPresence Resource Manager system can dynamically manage a HDX system or a RealPresence Group system, a user with the device administrator role must add a machine account for the system. This is the same username that the endpoint's system administrator should enter on the system for the provisioning service. This allows the Polycom endpoint and RealPresence Resource Manager system to authenticate and communicate without using a specific user's account.

The **Add Machine Account** dialog box includes the following information.

Field	Description
Enable Machine Account	Select or clear this option to enable and disable (respectively) the machine account you create for the endpoint.
Unlock Machine Account	Select this option to unlock machine accounts that become locked when they exceed the Failed login threshold. This will only happen when the password expires.
User ID	Enter a unique name for the machine account. As a best practice, name the machine account in a way that associates it with the corresponding device. For example, if your company names endpoint systems for the system user or room (for example, `bsmith_HDX` or `Evergreen_Room`), then give the machine account an associated **User ID** (`bsmith_HDX_machine` or `evergreen_room_machine`).
Password/ Confirm Password	Enter a password for the machine account user ID. This password must meet the **Local Password Requirements**. This password expires in 365 days.
Description	Enter a meaningful description for the endpoint.
Associate with an existing user or room	Select this option to associate the endpoint system with a specific user or room. This may be a local or enterprise user or room.
Associate with a new room (created automatically)	Select this option to associate the endpoint system with a system-generated room. The name of the new room is the same as the machine account **User Name** and can be edited when you edit the room. This option can only create a local room account. If you want to associate a machine account with an Active Directory account, you must first add the account through Active Directory.
Assign Area	When areas are enabled, you can assign the newly-created room to an area. Only users who manage more than one area can assign areas.

Once you have created this machine account on the RealPresence Resource Manager system, provide this information to the appropriate endpoint administrator. They should enter this **User ID** and **Password** as the **User Name** and **Password** on the **Provisioning Service** page.

Note that the machine account password expires after one year. After the expiration, the endpoint login will fail. After three failed login attempts, the system locks the machine account. You can reset the password and unlock the machine account by editing it and assigning a new password.

System Administration

Only users assigned the administrator role can perform general RealPresence Resource Manager system administration functions. The RealPresence Resource Manager system administration functionality and workflow changes when the system is running in maximum security mode. The following sections describe the areas of functionality and how they have changed.

Users assigned the administrator role can see the system **Dashboard**, the **Admin** menu, and the pages and **ACTIONS** associated with it.

Admin Menu

When the RealPresence Resource Manager system is in maximum security mode, the **Admin** menu in this release has changed in the following ways:

- On the **Server Settings** menu, the **Database**, **Calendaring Management**, **Remote Alert Setup** and **Email** menu options and their associated functionality have been removed.
- On the **Management and Security** menu, the **Security Options**, **Banner Configuration**, **Local User Account Configuration**, **Local Password Requirements**, and **Machine Accounts** menu options and their associated functionality have been added.

Direct Conference Templates

As was noted before, because all direct conferences scheduled on a RealPresence Resource Manager system running v7.3 must be hosted on a RMX conferencing system, the **MCU Settings** for all **Conference Templates** have changed in the following ways:

- The **Supported MCUs** section lists only **RMX** and cannot be changed.
- The **Always Use MCU** option on the **Conference Template** page is not available (grayed-out); it is always enabled and cannot be changed.

Provisioning Profiles

Because a RealPresence Resource Manager system running in maximum security mode supports only HDX systems and RealPresence Group systems running in dynamic management mode, the **Scheduled Provisioning Profiles** page and the **ACTIONS** associated with it are not available.

The **User Group Provisioning Profiles** page and the **ACTIONS** associated with it has not changed on a RealPresence Resource Manager system running in maximum security mode.

Software Updates

Because a RealPresence Resource Manager system running in maximum security mode supports only RealPresence Group series endpoints operating in dynamic management mode, the **Scheduled Software Update** page and the **ACTIONS** associated with it are not available.

The **Automatic Software Update** page and the **ACTIONS** associated with it do not change when the RealPresence Resource Manager is running in maximum security mode.

Server Settings

The **Server Settings** menu for a RealPresence Resource Manager system running in maximum security mode has changed significantly. The following options have been removed:

- Microsoft Lync or Office Communications Server Integration
- Redundant Configuration
- Remote Alert Setup
- E-mail

In addition, you will also note the following changes and additions:

- The **Network** settings page now includes the ability to enable IPv6 and to include a preferred and alternate DNS server.
- The **System Time** page does not include the **Minutes Between Synchronization** option when using an NTP server.
- On the **Enterprise Directory** page:
  - You must identify the enterprise directory by **DNS Name**. You can no longer identify the enterprise directory server by IP address.
  - The **Security Level** defaults to StartTLS and cannot be modified.
- The **Reclaim Inactive CMA Desktop Licenses** option has been removed from the **Licenses** page.
- The **CMA Desktop Logo** option has been removed from the **Custom Logo** page.

- The **Include dynamically-managed devices in the Global Address Book** option has been removed from the **Directory Setup** page.

Management and Security

A RealPresence Resource Manager system running in maximum security mode offers a new **Management and Security** workflow. The following sections describe the changes.

Security Options

The RealPresence Resource Manager system includes security options that cannot be modified when running in maximum security mode.

The only exception is that you can allow ping responses to the server if required.

Navigate to **Admin > Management and Security > Security Options** to view the security options.

Security Option	Can be enabled?
Allow XMPP (presence connections)	No
Allow ICMP (ping) responses	Yes
Respond to ICMP (ping) requests with Destination Unreachable message	Yes
Allow troubleshooting traces	No
Allow scheduling confirmation emails	No
Allow audio-only conferences	No
Allow non-LDAP directory protocols	No
Allow non-dynamically managed endpoints and point-to-point scheduling (unsecure dialout)	No
Allow remote alert emails	No
Allow Linux console access	No

Server Software Upgrade

The **Server Software Upgrade** workflow on a system running in maximum security mode does not change.

Certificate Management

Because a RealPresence Resource Manager system running in maximum security mode always operates in encrypted mode, the **Use HTTPS** is not an option on the Certificate Management page.

Session Management

The **Session Management** page allows an administrator to change but not disable the following settings:

Field	Description
Resource Manager user interface timeout	By default the RealPresence Resource Manager system user interface times out after 10 minutes of inactivity. Use this procedure to change the timeout value for the user interface inactivity timer. Possible value is 5 to 60 minutes.
Maximum number of sessions per user	The number of simultaneous login sessions per user ID. Possible value is 1 to 10 sessions.
Maximum number of sessions per system	The number of simultaneous login sessions by all users. Possible value is 2 to 50 sessions. **Note** If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to arrive is granted access, and the system terminates the non-Administrator session that's been idle the longest.

Banner Configuration

The **Banner Configuration** page allows users assigned the **Administrator** role to customize (but not disable) the long and short login banners.

A log in banner is the message that appears when users attempt to access the system. Users must acknowledge the message before they can log in.

By default, the long banner field on the **Banner Configuration** page displays the required Standard Mandatory Notice and Consent Provision for systems operating in a maximum security environment. The short banner field displays a shortened version of this same notice.

The long banner is used for the RealPresence Resource Manager system log in banner. It is also provisioned to endpoints that the RealPresence Resource Manager system manages. The short banner is provisioned to endpoints that the RealPresence Resource Manager system manages for those situations in which the long banner length exceeds the available display area.

The RealPresence Resource Manager system provides several sample long banners. You can use these banners as is or edit them to create a custom long banner. The RealPresence Resource Manager system provides a single short

banner, which you can also customize. If you customize the banners, remember that the long banner message may contain up to 5000 characters. The short banner message may contain up to 1315 characters.

Local User Account Management

The **Local User Account Management** page allows an administrator to change but not disable the following local user account settings:

Field	Description
Account Lockout	
Failed login threshold	Specify how many consecutive login failures cause the system to lock an account. Possible value is 2 to 10.
Failed login window (hours)	Specify the time span within which the consecutive failures must occur in order to lock the account. Possible value is 1 to 24.
Customized user account lockout duration (minutes)	Specify how long the user's account remains locked. Possible value is 1 to 480.
Account Inactivity	
Customize account inactivity threshold (days)	Specify the inactivity threshold that triggers disabling of inactive accounts. Possible value is 30 to 180.

Local Password Requirements

The **Local Password Requirements** page allows an administrator to change but not disable password security requirements by specifying password age, length, and complexity.

Field	Description
Password Management	
Maximum password age (days)	Specify at what age a password expires. Possible value is 30 to 180.
Minimum password age (days)	Specify how frequently a password can be changed. Possible value is 1 to 30.
Password warning interval (days)	Specify when users start to see a warning about their password expiration. Possible value is 1 to 7.
Minimum length	Specify the number of characters a password must contain. Possible value is 8 to 18.
Minimum changed characters	Specify the number of characters that must be different from the previous password. Possible value is 1 to 4.

Field	Description
Reject previous passwords	Specify how many of the user's previous passwords the system remembers and won't permit to be reused. Possible value is 8 to 16.
Password Complexity	
Lowercase letters	Specify the number of lowercase letters (a-z) that a password must contain. Possible value is 1 or 2.
Uppercase letters	Specify the number of uppercase letters (A-Z) that a password must contain. Possible value is 1 or 2.
Numbers	Specify the number of digit characters (0-9) that a password must contain. Possible value is 1 or 2.
Special characters	Specify the number of non-alphanumeric keyboard characters that a password must contain. Possible value is 1 or 2.
Maximum consecutive repeated characters	Specify how many sequential characters may be the same. Possible value is 1 to 4.

Reset System Passwords

The system has several underlying service passwords. The **Reset System Passwords** page allows an administrator to reset these underlying service passwords. When you select this option, all of these underlying service passwords will be changed to the same random system-generated value.

Whitelist

You can configure a whitelist of IP addresses that are allowed to access the RealPresence Resource Manager system's web interface or SNMP information.

When you enable the whitelist feature, only IP addresses included on the whitelist will be allowed to access the RealPresence Resource Manager system's web interface or SNMP information.

Network and Host Intrusion Detection

The RealPresence Resource Manager system has both HIDS (Host Intrusion Detection System) and NIDS (Network Intrusion Detection System) enabled at all times, regardless of security settings.

Network Intrusions

The RealPresence Resource Manager NIDS detects the following types of instrusions: a fast port scan, a slow port scan, a denial of service (DoS) attack, and a flood attack. These are currently defined as:

- Fast port scan:
  10 connections in a 5-second time period from the same source IP.
- Slow port scan:
  100 connections in a 1-hour time period from the same source IP.
- DoS attack:
  100 connections in a 5-second time period to the same destination port.
- Flood attack:
  100 connections in a 5-minute window to any destination port from any source IP.

If the RealPresence Resource Manager system detects an intrusion, it displays a system alert on the user interface. The alert text will indicate the type of intrusion detected, such as:

- Port scan detected. See kernal.log for details.
- DoS attack detected. See kernal.log for details.
- Flood attack detected. See kernal.log for details.

Host Intrusions

The HIDS monitors the internal file system of the RealPresence Resource Manager and will detect any changes made to it, specifically:

- file modification
- file creation
- file deletion
- file move
- file attribute change

Events logged by the HIDS are stored in a dedicated audit log called *hids.log*. When the HIDS is started during system initialization, the log file is initialized with a list of all monitored directories. After this, and changes result in a new log entry. Here are some examples:

Log File Initialization - Directory Monitored:

Aug 10 08:13:08 xma-120-78 inotify: [HIDS: watcher established] /usr/share/libvirt/schemas

File Created:

Aug 10 08:13:31 xma-120-78 inotify: [HIDS: entity created] /etc/sysconfig/iptables.KI3Mtw

File Modified:

Aug 10 08:13:31 xma-120-78 inotify: [HIDS: entity modified] /etc/sysconfig/iptables.KI3Mtw

File Attributes Changed:

Aug 10 08:13:31 xma-120-78 inotify: [HIDS: entity attributes modified] /etc/sysconfig/iptables.KI3Mtw

File Moved:

Aug 10 08:13:31 xma-120-78 inotify: [HIDS: entity moved] /etc/sysconfig/iptables.KI3Mtw moved to /etc/sysconfig/iptables

File Deleted:

Aug 10 08:13:32 xma-120-78 inotify: [HIDS: entity deleted] /opt/polycom/cma/7.3.0-117164/jserver/ads-work

Both the kernal.log and the hids.log files are available via the Reports > Audit Log Files menu via the RealPresence Resource Manager web UI. See the View and Download Audit Log Files section of the Polycom® RealPresence® Resource Manager System Operations Guide for details.

Troubleshooting

Troubleshooting Utilities

A RealPresence Resource Manager system running in maximum security mode has most of the same troubleshooting utilities of the standard commercial system; however the **Traces** functionality has changed and new functionality has been added. The following sections describe the troubleshooting utilities.

Resource Manager System Logs

There is no change in the **Resource Manager System Logs** function.

Test Network Connect

The **Test Network Connect** function allows you to perform a **Traceroute** or **Ping** operation. **Traceroute** allows you to investigate the route path and transit times of packets as they travel across an IP network. **Ping** allows you to test the availability of a host on an IP network.

Systems

The **Systems** pane displays summary information about the devices that access the RealPresence Resource Manager system. For a RealPresence Resource Manager system running in maximum security mode, systems are limited to **Endpoints**, **MCUs**, and **Rooms**.

Resource Manager Configuration

The **Resource Manager Configuration** pane displays information about the configuration of the system. For a system running in maximum security mode, configuration items are limited to **Software Version**, **Hardware Version**, **Number of Processors**, **Enterprise Directory**, **Database**, **Time Source**, and **Enterprise Directory DC** (Domain Controller).

Resource Manager Info

The **Resource Manager Info** pane displays general information about the RealPresence Resource Manager system. For a RealPresence Resource Manager system running in maximum security mode, this includes the following:

- Standard information:
  CPU Utilization, Paging File Utilization, Last Hard Start/Reboot, Provisioning Operations in Progress operations, Software Update Operations in Progress, Hardware Alarms, Threshold Alarms, Temperature, Power Supply Status, Battery Status, and Cooling Fan Status, Total Memory, Free Memory, and Partition States.

Resource Manager Licenses

There is no change in the **Resource Manager Licenses** function.

Users Logged-In

The **Users Logged In** pane displays the type and number of users that are currently logged into the system.

Report Administration

The only **Report Administration** function supported on a RealPresence Resource Manager system running in maximum security mode is the **Retention Period to keep Conference and Endpoint CDRs (in Days)**. All other **Report Administration** functions including creating and storing a weekly archive of the CDRs is not available when running in maximum security mode.