TN1303704

MILITARY UNIQUE DEPLOYMENT GUIDE

10.0.1 | November 2016| 3725-72113-001A2

RealPresence® Resource Manager

6001 America Center Drive
San Jose, CA 95002
USA

Contents

About this Guide

This guide provides the setup information that you need to install and configure a Polycom RealPresence Resource Manager system in a high security environment.

Audience, Purpose, and Required Skills

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

Documentation Resources

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

- *Polycom RealPresence Resource Manager System Operations Guide*
- *Polycom RealPresence Resource Manager System Web Scheduling Guide*
- *Polycom RealPresence Resource Manager System Getting Started Guide*
- *Polycom RealPresence Resource Manager System Upgrade Guide*
- *Polycom RealPresence Resource Manager System Release Notes*

The latest documentation is on the RealPresence Resource Manager support site.

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	Build Version	Certification Date	Description
1.0	GS 4.1.0_J and RPRM 7.3.0J	February, 2014	Initial Certification with Redcom for Group Series and RP Resource Manager
2.0	GS 4.1.5	April, 2015	DTR1 – Updated GS features, added fixes, addressed POA&Ms
3.0	GS 4.1.5	April, 2015	DTR2 – Shift GS to AEI Listing after testing with NEC
4.0	GS 4.3.0	July, 2015	DTR3 – Updated GS features, added fixes
5.0	GS 4.3.2	October, 2015	DTR4 – Added GS310, EEP Camera

Doc Version	Build Version	Certification Date	Description
6.0	GS and Centro 5.1.2	October, 2016	DTR5 – Updated GS features, added fixed, added Centro Platform
7.0	RPRM 10.0.1	November 2016	DTR6 – Updated RPRM to 10.0.1

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

Conditions of Fielding

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 (DAA):

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:

- Application Security and Development Checklist:
  - APP3305, CAT I, for RPRM
  - APP3280, CAT II, for RPRM
  - APP3290, CAT II, for RPRM
  - APP3300, CAT II, for RPRM
- Application Services Checklist:
  - APS0110, CAT II, for RPRM
- Defense Switched Network (DSN):
  - DSN13.17, CAT II (x6), for RP Centro, RPGS 300, RPGS 310, RPGS500, RPGS700, and RPRM
- Network Checklists:
  - NET0445, CAT II (x6), for RP Centro, RPGS 300, RPGS 310, RPGS 500, RPGS 700, and RPRM

b The site must use role-based security for user access and management of the vendor's device.

c The system must be integrated into the site's AD environment for normal user access, authentication, and authorization requirements.

d The site must disable all local user accounts on the device after initial setup/configuration with the exception of one emergency administrative account.

e The site must ensure that the emergency administrative account's userid and password are locked up in separate safes, both of which are not accessible by any one individual, and procedures are implemented to log all accesses and usages.

f The site must ensure that the emergency administrative account meets all DoD userid and password complexity requirements.

g The site must ensure all unused ports are closed.

h The site must be a STIG-compliant and CAC-enabled workstation for management of the solution.

i The configuration must be in compliance with the Polycom RPGS Family Rel. 5.1.2 military-unique features deployment guide.

- 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.

Get Help

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

Polycom and Partner Resources

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

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 on-line 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.

Deploy RealPresence Resource Manager in a Military Unique Environment

You can make your system work in a high security environment by configuring the options described in this section.

Before this, you need to install and set up your system by finishing the tasks documented in *RealPresence Resource Manager Getting Started Guide*.

Complete the following tasks to deploy the RealPresence Resource Manager system in a high security environment.

- Set NTP Server
- Install CA Signed Certificates
- Customize the Banner Message
- Edit the Provisioning Profiles
- Edit the Provisioning Profiles

Set NTP Server

NTP server is used to verify the time of CA certificate. Configure your system time to make it synchronize with an external NTP server. Make sure that the RealPresence Resource Manager system and the components that it manages use the same NTP server.

For more information on setting NTP server, see **Time Settings** in *RealPresence® Resource Manager Operations Guide*.

Apply High Security Settings Baseline

The system comes with **High Security Settings Baseline** ready for a maximum level of security. You should use the high security baseline settings only when you require maximum levels of security.

To apply High Security Settings Baseline:

1. Go to **Admin > Management And Security** > **Security Baseline.**
2. Select **High Security Settings Baseline**.
3. Select **MORE > Apply Baseline**.

   The system will reboot.

High Security Baseline Settings

After you apply **High Security Settings Baseline**, the **SSH Access** is set to **Disabled Permanently**. This setting becomes read-only and you cannot change it back.

Secure Communication Settings

Field	Enabled?
HTTP: Enforce Secured http	Yes **Inbound:** true **Outbound:** true
LDAP: Enforce Secured LDAP	Yes **Inbound:** true **Outbound:** true
FTP: Enforce Secured FTP	Yes **Inbound:** true **Outbound:** true
SMTP: Enforce Secured SMTP	Yes
SNMP: Enforce Secured SNMP v3	Yes
Disable GDS (Global Directory Service)	Yes
Disable Outbound Telnet	Yes

TLS Settings

Field	Enabled
Cipher Mode	Strong Ciphers
Enabled Protocols	TLS1.2: false TLS1.1: true TLS1.0: true SSLv3: false
Validate Certificates for Connections from Clients	Yes
Validate Certificates for Connections to Servers	Yes
Verify Hostname	Yes Select **Yes** to verify the host name (IP address) of the server. With **Verify Hostname** enabled, IP address will be used to validate the CA certificate of RealPresence Resource Manager. Therefore the SAN must contain the IP address of the server (RealPresence Resource Manager); otherwise, verifying host name will fail.

Field	Enabled
Enable FIPS -140	Yes
Check Revocation Status	Yes

System Hardening Settings

Field	Enabled?
Enable NIDS	Yes
Ignore Redirect Flag	Yes
Allow ICMP (ping) responses	No
Respond to ICMP (ping) requests with Destination Unreachable message	No
Allow traces for troubleshooting	No
Allow Linux console access	No
Disable Root User Login	Yes
SSH Access	Disabled Permanently
Lock Bios	Yes

Session Management Settings

Field	Enabled?
RealPresence Resource Manager user interface timeout (minutes)	Yes User interface timeout is set for 10 minutes.
Maximum number of sessions per user	Yes Maximum number of sessions per users is set to 5.
Maximum number of sessions per system	Yes Maximum number of sessions is set to 50.
Enable Banner	Yes

User Account Configuration

Field	Enabled?
Account Lockout	
Failed login threshold	Yes Threshold is set to 3 failed attempts.
Failed login window (hours)	Yes Time span is set to 1 hour.
Customized user account lockout duration (minutes)	No

Field	Enabled?
Account Inactivity	
Customize account inactivity threshold (days)	Yes Threshold is set to 30 days.

Password Requirements

Field	Enabled?
Password Management	
Minimum length (characters)	Yes Minimum length is 15 characters.
Minimum changed characters	Yes Minimum number of changed character is 4.
Minimum password age (days)	Yes Password can be changed only once per day.
Maximum password age (days)	Yes Password expires after 60 days.
Minimum system password age (days)	Yes Password expires after 360 days
Password warning interval (days)	Yes Password warning interval is set to 7 days.
Reject previous passwords	Yes Previous 10 passwords will be rejected.
Password Complexity	
Lowercase letters	Yes Two lowercase letters are required.
Uppercase letters	Yes Two uppercase letters are required.
Numbers	Yes Two digits are required.
Special characters	Yes Two special characters are required.
Maximum consecutive repeated characters	Yes Only two repeated characters are allowed.
OS Account Password Policy	
Apply rules to the OS account	No
Conference PIN Code	

Field	Enabled?
Minimum length	Yes Minimum length is 9 characters.
Maximum length	Yes Maximum length is 16 characters.
Maximum consecutive repeated characters	Yes Only two consecutive repeated characters are allowed.

For more information on security baseline settings, see **Securing the System** in *RealPresence® Resource Manager Operations Guide*.

Install CA Signed Certificates

Polycom recommends you to install CA signed DoD PKI certificates other than self-signed certificates to improve system security.

To configure and use CA signed DoD PKI:

1. Create a Certificate Signing Request (CSR) and have it signed by the CA that issues certificates for the particular PKI within your environment.

   After you apply the **High Security Settings Baseline**, the **Validate Certificates for Connections from Clients**, **Validate Certificates for Connections to Servers**, and **Verify Hostname** options are enabled to validate certificates and the host name (IP address) of the server.

   With **Verify Hostname** enabled, IP address will be used to validate the CA certificate of RealPresence Resource Manager. Therefore the SAN in your CSR must contain the IP address of the server (RealPresence Resource Manager); otherwise, verifying host name will fail.
2. Install the CA signed certificate into the RealPresence Resource Manager system.
3. View Certificates and Certificate Details from the RealPresence Resource Manager GUI.

For more information on configuring certificates, see **Security Certificates** in *RealPresence® Resource Manager Operations Guide*.

Customize the Banner Message

The banner message appears when users attempt to access the system. Users must acknowledge the message before they can log in. The RealPresence Resource Manager system provides several sample long banners. The **Sample 1** message is designed for high security system. You can either use it or customize a banner message based on **Sample 1**.

Enable Banner

You must enable banner to show the message when you log into the system.

To enable banner:

1. Go to **Admin > Management and Security Settings > Session Management.**
2. Select the **Enable Banner** check box.
3. Click **Update**.

Edit Banner Message

The **Banner Configuration** page allows users assigned the Administrator role to customize the long and short login banners.

To edit the login banners:

1. Go to **Admin > Management and Security Settings > Banner Configuration**.
2. From the **Message** drop-down menu, select the **Sample 1** banner. You can also edit the banner as needed. If you edit the existing banners, the **Message** menu selection changes to **Custom**.
3. Click **Update**.

For more information on changing the banners, see **Session Security and User Access** in *RealPresence® Resource Manager Operations Guide*.

Edit the Provisioning Profiles

You can improve the security of the communication between the RealPresence Resource Manager system and the endpoints that it provisions by configuring the security settings of the provisioning profiles.

This section lists the recommended settings for the **Default Admin Config Provisioning Profile** and **Default Network Provisioning Profile** that you can use to configure a high security system.

For more information on provisioning profile settings, see **Working with Provisioning Profiles** in *RealPresence® Resource Manager Operations Guide*.

To Edit the Default Network Provisioning Profile:

1. Go to **Endpoint > Dynamic Management > Provisioning Profiles**.
2. Select **Default Network Provisioning Profile** and click .
3. Edit the following settings under the **Security Settings**, **Security Settings 2**, and **Directory Settings** tabs according to the recommended values in the table below.

Recommended Settings for Default Network Provisioning Profile

Field	Recommended Value
Security Settings	
Security Profile	Ultra
Enable Dynamic Provisioning for ID/Passwords	Checked
Enable Secure Mode	Checked

Recommended Settings for Default Network Provisioning Profile

Field	Recommended Value
Enable HTTPS Only	Checked
Security Settings 2	
Lock Port after Failed Logins	3
Enable NIDS	Checked
Directory Settings	
Verify Certificate	Checked

4 Click **OK.**

To Edit the Default Admin Config Provisioning Profile:

1 Go to **Endpoint > Dynamic Management > Provisioning Profiles**.
2 Select **Default Admin Config Provisioning Profile** and click .
3 From the **System Settings** tab, clear the **Recent Calls** check box.
4 Click **OK**.