Polycom Unified Communications Deployment Guide for Polycom® RealPresence® Mobile Systems in H.323 Environments
About This Guide

This guide describes how to configure the necessary network components and surrounding DNS infrastructure required for using Polycom® RealPresence® Mobile in a corporate H.323 environment.

This guide does not discuss considerations for deploying RealPresence Mobile in SIP environments.

The following components are discussed:

- Polycom Converged Management Application™ (CMA®)
- Polycom Distributed Media Application™ (DMA™)
- Polycom RMX® systems
- Polycom Video Border Proxy™ (VBP®)
- Polycom RealPresence® Mobile

Other products can also be used in a RealPresence solution. Note that there are multiple ways to deploy RealPresence Platform infrastructure, and your environment might be different from what is described here. For complex deployments, contact your Polycom Account Manager to discuss Professional Services options.

For help using RealPresence Mobile and information about specific software versions, go to support.polycom.com.

Related Documentation

For detailed information about a specific Polycom product, refer to the product documentation for that product. You can find Polycom product documentation online at support.polycom.com.
Required Skills

Integrating Polycom RealPresence Mobile with the Polycom infrastructure requires planning and knowledge of the basics of video conferencing standards and networking. In order to deploy RealPresence Mobile, you should also understand DNS, Active Directory, and Firewalls.

Polycom Solution Support Services

For customer support, visit the RealPresence Mobile User community at community.polycom.com.

For customer support on Polycom service-entitled equipment, you can enter a service request by contacting Polycom Global Services at support.polycom.com.

You can find additional support contact information at support.polycom.com/PolycomService.
Contents

1 Polycom Unified Communications with RealPresence Mobile  . 1
   Supported Deployment Models .................................................. 1
   Polycom CMA System as H.323 Gatekeeper .......................... 1
   Polycom DMA System as H.323 Gatekeeper ......................... 1
   Supported Products ................................................................. 2

2 Polycom CMA System as H.323 Gatekeeper  ............... 3
   Deployment Model Advantages ................................................. 3
   Deployment Architecture ......................................................... 4
   Device Licensing ................................................................. 5
   CMA Seat Licenses for RealPresence Mobile .......................... 5
   Reclaiming Licenses ............................................................... 6
   Solution Overview ................................................................. 6
   Configuring the DNS Service .................................................. 6
   Task Overview ................................................................. 7
   Configuring the CMA System ................................................. 11
   Task Overview ................................................................. 11
   Configuring the VBP-ST System ............................................ 14
   Task Overview ................................................................. 14
   Configuring the RMX System ............................................... 17
   Task Overview ................................................................. 18
   Configuring the RealPresence Mobile Systems ..................... 18
   Task Overview ................................................................. 19

3 Polycom DMA System as H.323 Gatekeeper  ............... 21
   Deployment Model Advantages ................................................. 21
   Deployment Architecture ......................................................... 22
   Device Licensing ................................................................. 23
   CMA Seat Licenses for RealPresence Mobile .......................... 23
   DMA Licenses for RealPresence Mobile .................................. 24
   Solution Overview ................................................................. 24
   Configuring the DNS Service .................................................. 24
   Configuring the CMA System ................................................. 24
   Task Overview ................................................................. 25
   Configuring the DMA System ................................................. 26
   Task Overview ................................................................. 26
   Configuring the VBP-ST System ............................................ 27
   Task Overview ................................................................. 28
   Configuring the RMX System ............................................... 29
   Configuring the RealPresence Mobile Systems ..................... 29
4 Capacity Planning ............................................. 31
  RealPresence Mobile User Models .................................. 31
  Estimating Server Capacity ........................................ 32
  Calculating Capacity ............................................. 33
    Variables ......................................................... 33
    Formulas ....................................................... 34
Polycom Unified Communications with RealPresence Mobile

Polycom’s integrated suite of hardware devices and software applications enables you to integrate high-quality video and audio communications using mobile devices such as tablets and smartphones.

Supported Deployment Models

The ideal network setup for using Polycom RealPresence Mobile for H.323 environments depends on your organization’s size, your existing deployment, and your preferences for high availability versus cost of investment.

Two reference solutions are provided in this guide to show the typical architecture:

- Polycom CMA System as H.323 Gatekeeper
- Polycom DMA System as H.323 Gatekeeper

Polycom CMA System as H.323 Gatekeeper

In this model, Polycom CMA system works as the provisioning server, directory server, and H.323 gatekeeper to provide the call signaling service for RealPresence Mobile systems.

Polycom DMA System as H.323 Gatekeeper

In this model, the Polycom DMA 7000 system works as H.323 gatekeeper to provide call signaling service for RealPresence Mobile systems. The DMA also enables you to manage your multipoint conference unit (MCU) resources.

A Polycom CMA system is also needed to provide the provisioning service.
Supported Products

The following table lists the product versions that are discussed in this guide and supported by RealPresence Mobile Version 1.1.


<table>
<thead>
<tr>
<th>Product Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence Mobile for Android</td>
<td></td>
</tr>
<tr>
<td>• Motorola XOOM</td>
<td>Version 1.1</td>
</tr>
<tr>
<td>• Samsung Galaxy Tab</td>
<td></td>
</tr>
<tr>
<td>• Motorola DROID XYBOARD</td>
<td></td>
</tr>
<tr>
<td>Polycom RealPresence Mobile for iOS</td>
<td></td>
</tr>
<tr>
<td>• iPad 2</td>
<td>Version 1.1</td>
</tr>
<tr>
<td>• iPhone 4S</td>
<td></td>
</tr>
<tr>
<td>Polycom VBP 5300-ST</td>
<td>Version 11.2.6</td>
</tr>
<tr>
<td>Polycom VBP 6400-ST</td>
<td></td>
</tr>
<tr>
<td>Polycom RMX 4000</td>
<td>Version 7.6.0</td>
</tr>
<tr>
<td>Polycom RMX 2000</td>
<td></td>
</tr>
<tr>
<td>Polycom DMA 7000</td>
<td>Version 4.0.3</td>
</tr>
<tr>
<td>Polycom CMA 5000</td>
<td>Version 6.0.1</td>
</tr>
<tr>
<td>Polycom CMA 4000</td>
<td></td>
</tr>
<tr>
<td>Microsoft Active Directory</td>
<td>Windows Server 2008 R2 enterprise</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Windows Server 2008 R2 enterprise</td>
</tr>
</tbody>
</table>
Polycom CMA System as H.323 Gatekeeper

In this deployment model, the Polycom CMA system functions as the provisioning server, directory server, and H.323 gatekeeper.

**Deployment Model Advantages**

A single CMA system provides provisioning and call signaling services. This deployment model is cost-effective for small organizations with a small number of endpoints and MCU resources to manage.

Refer to **Formulas** for more information about server capacity.
Deployment Architecture

The following figure illustrates the reference architecture for this deployment model.
Function | Description
--- | ---
Authentication and Provisioning | The Polycom CMA system provides authentication and provisioning services to RealPresence Mobile systems. Authentication can be performed by the CMA system locally or through the organization’s Active Directory server.

Directory | The CMA system provides global directory service to RealPresence Mobile systems through either the local directory or the organization’s Active Directory server.

Device Management | The CMA system can perform limited monitoring of the RealPresence Mobile systems, such as online, offline, in-call, and bandwidth management, but it does not support automatic software updates for RealPresence Mobile systems.
The CMA system can provide call reports, such as Call Detail Records.

Registration and Call Control | H.323 registration and call control services are provided by the CMA system.

Access from an External Network | The Polycom VBP-ST system provides the firewall traversal service when RealPresence Mobile systems access the CMA system from an external network (Internet).
If there is an existing VPN deployment for Internet access, RealPresence Mobile systems can access the CMA system through VPN connect.

Video Conference | Polycom RMX systems provide audio and video conference service for the RealPresence Mobile system.

Split DNS | Split DNS enables RealPresence Mobile systems to use the identical SRV record or Fully-Qualified Domain Name (FQDN) from both internal and external networks (Internet).

DNS Load Balancing | Deploying more than one VBP-ST system can provide load balancing through the DNS configuration when RealPresence Mobile systems access from an external network (Internet).

**Device Licensing**

**CMA Seat Licenses for RealPresence Mobile**

The number of CMA seat licenses used by RealPresence Mobile varies among different use cases.
Periodically, CMA system administrators may need to manually reclaim licenses that are no longer being used.

1. In the Endpoint Monitor View, filter by Type to show only the RealPresence Mobile endpoints.
2. Sort the records by Status.
3. Select offline RealPresence Mobile systems, and click **Delete**.

### Solution Overview

The following tasks are required for deploying RealPresence Mobile in an environment that uses CMA as the H.323 gatekeeper.

1. Configuring the DNS service.
2. Configuring the CMA system.
3. Configuring the VBP-ST system.
4. Configuring the RMX system.
5. Configuring the RealPresence Mobile systems.

### Configuring the DNS Service

To enable RealPresence Mobile systems using identical FQDNs from both internal and external networks, split DNS should be configured. To support the Auto Find Provisioning Server feature, the SRV record must be configured.

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>Number of Licenses Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>One user signs in from one device</td>
<td>1 license</td>
</tr>
<tr>
<td>Multiple users sign in from the same device</td>
<td>1 license per user</td>
</tr>
<tr>
<td>One user signs in from multiple devices</td>
<td>1 license per device</td>
</tr>
</tbody>
</table>
This guide discusses necessary procedures for supporting RealPresence Mobile deployment. It is assumed that both internal and external DNS servers are already set up and configured for the corporate domain.

**Task Overview**

Perform the following steps to create DNS address records on the DNS server.

1. Create DNS A record on the external DNS server.
2. Create DNS SRV record on the external DNS server.
3. Create DNS A record on the internal DNS server.
4. Create DNS SRV record on the internal DNS server.
5. Validate DNS settings on the external DNS server.
6. Validate DNS settings on the internal DNS server.

**Task 1: Create DNS A record on the external DNS server**

The DNS A record on external DNS server maps the FQDN of the VBP-ST system to its Internet IP address. Each VBP-ST system needs one FQDN.

The following example uses the configurations for Windows Server 2008 R2 enterprise as DNS server.

1. Select the domain example.com (where example.com is the existing domain name of the enterprise).
2. Right-click on the domain, and select **New Host (A or AAAA)** to add A records.

   For example, if there are two VBP-ST systems with the FQDN name corp1.example.com and corp2.example.com, and their Internet IP addresses are 172.16.13.14 and 172.16.13.15, add two A records as follows:

   **A Record 1:**
   Name = corp1
   IP address = 172.16.13.14

   **A Record 2:**
   Name = corp2
   IP address = 172.16.13.15
Task 2: Create DNS SRV record on the external DNS server

The SRV record on the external DNS server maps the SRV service address to the FQDN of the VBP-ST system.

The SRV record is required by the Auto Find Provisioning Server feature on RealPresence Mobile.

The following example uses the configurations for Windows Server 2008 R2 enterprise as the DNS server.

1. Select the domain example.com (where example.com is the existing domain name of the enterprise).

2. Right-click on the domain, and select Other New Records..., and then select Service Location (SRV) to create the SRV record.

For example, if there are two VBP-ST systems with the FQDN name corp1.example.com and corp2.example.com, add two SRV records as follows:

SRV Record 1:
Service = _cmaconfig
Protocol = _tcp
Priority = 0
Weight = 50
Port = 443
Host offering this service = corp1.example.com

SRV Record 2:
Service = _cmaconfig
Protocol = _tcp
Priority = 0
Weight = 50
Port = 443
Host offering this service = corp2.example.com

Weight = 50 means that each VBP-ST FQDN is returned randomly with 50% possibility for SRV query _cmaconfig._tcp.example.com. Therefore, two VBP-ST systems balance the traffic from the Internet.

Task 3: Create DNS A record on the internal DNS server

The CMA system in the internal network needs one A record to map its FQDN to the IP address on the internal DNS server.
Optionally, the RealPresence Mobile system can use a specified FQDN as the provisioning server, rather than using the Auto Find Provisioning Server setting. To support Split DNS, one VBP-ST system requires one A record to map to the CMA system’s IP address.

The following example uses the configurations for Windows Server 2008 R2 enterprise as DNS server.

1. Select the domain example.com (where example.com is the existing domain name of the enterprise).

2. Right-click on the domain, and select **New Host (A or AAAA)** to add A record.
   
   For example:
   - if the CMA system's FQDN is cma.example.com
   - its internal network IP is 10.11.12.13
   - and there are two VBP-ST systems with the FQDN names corp1.example.com and corp2.example.com
   
   then add three A records as follows:
   
   **A record 1:**
   
   Name = cma
   
   IP address = 10.11.12.13
   
   **A record 2:**
   
   Name = corp1
   
   IP address = 10.11.12.13
   
   **A record 3:**
   
   Name = corp2
   
   IP address = 10.11.12.13
   

**Task 4: Create DNS SRV record on the internal DNS server**

The SRV record on the internal DNS server maps SRV service to the FQDN of the CMA system.

The following example uses the configurations for Windows Server 2008 R2 enterprise as the DNS server.

1. Select the domain example.com (where example.com is the existing domain name of the enterprise).

2. Right-click on the domain and select **Other New Records...**, and then select **Service Location (SRV)** to create the SRV record.
For example, if cma.example.com is the FQDN of the CMA system, add one SRV record as follows:

SRV Record:
- Service = _cmaconfig
- Protocol = _tcp
- Priority = 0
- Weight = 100
- Port = 443
- Host offering this service = cma.example.com

**Task 5: Validate DNS settings on the external DNS server**

The following steps use the Windows nslookup command as an example. The procedure is similar on Mac and Linux.

1. From a Windows computer located on the Internet network, open a command line.
2. Type `nslookup corp1.example.com` to check the A record of the VBP-ST system. The response should include the corresponding VBP-ST system's Internet IP address.
   
   Do the same against `corp2.example.com`.
3. Type `nslookup -type=srv _cmaconfig._tcp.example.com` to check the SRV record. The response should include the FQDN of each VBP-ST systems.
   
   Enter the same command. The order of returned FQDNs should be changed.

**Task 6: Validate DNS settings on the internal DNS server**

The following steps use the Windows nslookup command as an example. The procedure is similar on Mac and Linux.

1. From a Windows computer located on the internal network, open a command line.
2. Type `nslookup cma.example.com` to check the A record of the CMA system. The response should include the CMA system's IP address.
   
   Do the same for `corp1.example.com` and `corp2.example.com`. The response should include the CMA system's IP address.
3. Type `nslookup -type=srv _cmaconfig._tcp.example.com` to check the SRV record. The response should include the FQDN of the CMA system.
Configuring the CMA System

The following deployment procedure includes necessary steps for enabling RealPresence Mobile usage on a CMA system. You must set up the CMA system and enable licenses in advance for the CMA system.


Task Overview

1. Configure CMA system as H.323 gatekeeper.
2. Edit site topology.
3. Create user accounts for RealPresence Mobile.
4. Set up provisioning for RealPresence Mobile.

Task 1: Configure CMA system as H.323 gatekeeper

1. To log in to a CMA system, in a browser enter the CMA system IP address or host name.

2. Go to Admin > Gatekeeper Settings > Primary Gatekeeper.
   The following screen is displayed.

<table>
<thead>
<tr>
<th>Gatekeeper Identifier:</th>
<th>Example Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatekeeper Description:</td>
<td>Example Description</td>
</tr>
<tr>
<td>Default Gatekeeper:</td>
<td>✓</td>
</tr>
<tr>
<td>Allow Registration of:</td>
<td>All Endpoints</td>
</tr>
<tr>
<td>Registration Refresh (seconds):</td>
<td>300</td>
</tr>
<tr>
<td>Maximum Neighbor Gatekeeper Hop Counts:</td>
<td>5</td>
</tr>
<tr>
<td>Log calls to/from unregistered endpoints:</td>
<td>✓</td>
</tr>
<tr>
<td>Deny calls to/from unregistered endpoints:</td>
<td></td>
</tr>
<tr>
<td>Enable Real-Time Statistics:</td>
<td></td>
</tr>
<tr>
<td>IRR Frequency (seconds):</td>
<td>0</td>
</tr>
<tr>
<td>Call Model:</td>
<td>Routed Mode</td>
</tr>
</tbody>
</table>

Update
3 Complete the following fields.

- In the **Gatekeeper Identifier** field, enter a gatekeeper name.
- In the **Gatekeeper Description** field, enter a description for the gatekeeper.
- In the **Call Model** field, select Routed mode.
- Select the default values for all other fields.
- Click **Update**.

**Task 2: Edit site topology**

In general, a CMA system uses a site to manage devices that are located in different geographical areas. A site contains one or more network subnets, and a device’s IP address identifies the site to which it belongs. Usually, the RealPresence Mobile system that uses the same provisioning is put into the same site.

The RealPresence Mobile systems in a site can always call each other. To enable calling systems in another site, you must configure the site link or network cloud. You can also configure the bandwidth control on each site and site link.

If the site topology (sites, site links, or network cloud) has already been created, you can use the existing topology for deploying RealPresence Mobile.

Refer to the *Polycom CMA System Version 6.0 Operations Guide* for details about the configuration of site, site links, network cloud, and bandwidth control, available at support.polycom.com.

**Task 3: Create user accounts for RealPresence Mobile**

You can create RealPresence Mobile user accounts locally on the CMA or integrate with the enterprise Active Directory server. Both types of user accounts can use directory search on RealPresence Mobile systems.

For information on integrating with the enterprise Active Directory server, refer to the *Polycom CMA System Version 6.0 Operations Guide*, available at support.polycom.com.

To create a local user account, go to **User > Users**, click **Add**, and enter the necessary information.
Task 4: Set up provisioning for RealPresence Mobile

To set up provisioning for RealPresence Mobile, you must configure both site provisioning and automatic provisioning. Site provisioning includes H.323, security, and firewall settings. Automatic provisioning includes settings that specify call speeds.

1. Configure site provisioning for a site that does not include your VBP-ST.
   a. Go to Admin > Dial Plan and Sites > Sites.
   b. In the Site list, select the site that includes the RealPresence system, and select Edit Site Provisioning Details.
   c. In the H.323 Settings pane, select Enable IP H.323, and then select This Server.
   d. In the Security Settings pane, select When Available for AES Encryption.
   e. Edit other site provisioning settings as needed, and click OK.

2. Configure site provisioning for a site that includes your VBP-ST system exclusively.
   You must also ensure that Enable H.460 Firewall Traversal is enabled in Firewall Settings.

3. Configure automatic provisioning.
   a. Go to Admin > Provisioning Profile > Automatic Provisioning Profiles.
   b. In the Automatic Provisioning Profile page, click Add, and enter a name for the provisioning profile.
   c. Go to H.323 Settings.
Set the **Maximum Speed for Receiving Calls (Kbps)** field and the **Preferred Speed for Placing Calls (Kbps)** field.

<table>
<thead>
<tr>
<th>Maximum Speed for Receiving Calls (Kbps)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Calls</td>
<td>384</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Preferred Speed for Placing Calls (Kbps)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Calls</td>
<td>512</td>
</tr>
</tbody>
</table>

To apply the provisioning profile to RealPresence Mobile users, follow these steps:

1. Create a group.
2. Associate the profile with the group.
3. Assign the user to the group.

### Configuring the VBP-ST System

Deploying the Polycom Video Border Proxy (VBP) ST series as access proxy makes it possible for endpoints outside the corporate network to register to the corporate CMA system and communicate with endpoints registered to the same system.

**Task Overview**

The recommended deployment strategy is to use the VBP-ST series in parallel with corporate firewalls, which means the external interface of VBP-ST is directly connected to the Internet.

This guide covers only the necessary steps to support deployment of RealPresence Mobile. For detailed configuration information, additional options, and other VBP-ST deployment strategies, refer to the *Polycom VBP Configuration Guide*, available at [support.polycom.com](http://support.polycom.com).

1. Configure VBP-ST network settings.
2. Configure CMA system to collaborate with VBP-ST.
3. Configure VBP-ST system to collaborate with CMA.
4. Validate the configuration.
Task 1: Configure VBP-ST network settings

1. In the VBP web interface, go to Configuration Menu > Network.
2. Configure the Subscriber Interface, which is the external interface facing the Internet.
3. Configure the Provider Interface, which is the internal interface facing the corporate network.
4. Configure the Default Gateway.
5. Configure DNS Servers.
6. (Optional) Configure other settings as needed.

Task 2: Configure CMA system to collaborate with VBP-ST

1. Add VBP-ST in the CMA system.
   a. In the CMA system’s web interface, go to Network Device > VBP.
   b. Click Add, and enter the Name, Provider-side IP, and Subscriber-side IP for the VBP system.
2. Copy the CMA certificate to the VBP-ST system.
   a. Ensure that the CMA system can connect to the VBP-ST system’s provider interface.
   b. In the CMA system’s web interface, go to Network Device > VBP.
   c. Select the VBP, and click Copy Certificate to VBP.
   d. Enter the file name of the certificate and the account credentials needed to access the VBP via SSH2.

Contact the VBP administrator if you need root credentials.

The CMA certificate is automatically copied to the VBP-ST. To view the certificate, go to Configuration Menu > Security > Access Proxy Certificates in the VBP web interface.

3. Configure the CMA site for VBP-ST.
   This example shows one way to configure the site on the CMA system for VBP-ST devices.
   a. In the CMA system’s web interface, go to Admin > Dial Plan and Sites > Sites.
   b. Click Add, and enter the Site Name, Description, and VBP Provider-side IP addresses to the subnet.
   c. Select the site, and click Edit Site Provisioning Details.
d  Go to Firewall Settings, and select Enable H.460 Firewall Traversal.

e  Go to H.323 Settings, and select Enable IP H.323, and then choose This Server.

e  Go to Security Settings, and select When Available for AES Encryption.

If there are multiple VBP-ST systems deployed in the network, they can be in the same site or different sites, as long as the Site Provisioning Details are correctly configured.

When registering to the CMA system through VBP-ST, RealPresence Mobile systems use the provisioning details of the CMA site defined for VBP-ST.

Task 3: Configure VBP-ST system to collaborate with CMA

1  Configure the VBP-ST VoIP ALG H.323 settings.

   a  In the VBP web interface, go to Configuration Menu > VOIP ALG > H.323.

   b  In Gatekeeper mode, select WAN/Provider-side gatekeeper mode.

   c  Enter the IP address of the CMA server as the WAN/Provider-side GK address.

   d  Enable H.460.18 support.

   e  (Optional) Configure other settings as needed.

2  (Optional) Add Access Proxy Certificates.

The VBP is pre-installed with self-signed certificates to configure the Access Proxy. These certificates can be replaced with Signed certificates issued by a certificate authority (CA). Access Proxy can have different certificates for each protocol, making the SSL encryption different for each service.

   a  In the VBP web interface, go to Configuration Menu > Security > Access Proxy Certificates.

   b  Add certificates as needed.

The VBP-ST system includes two sets of certificates:
•   Access Proxy certificates located at Security > Access Proxy Certificates
•   VOIP Traversal certificates located at Security > Certificate Store

3  Configure the VBP system’s HTTPS service to use an alternate HTTPS port.

   a  In the VBP web interface, go to Configuration Menu > Security > HTTPS Configuration.
b Set the Alternate HTTPS port to a value other than 443, for example, 445.

By default, the VBP system’s own HTTPS service and the HTTPS Access Proxy use port 443. Therefore, you must configure the VBP system’s HTTPS service to use an alternate port.

4 Configure the VBP-ST for access proxy.
   a In the VBP web interface, go to Configuration Menu > System > Access Proxy.
   b Enable Access Proxy.
   c Add the following access proxies.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>LDAP</td>
<td>389</td>
</tr>
<tr>
<td>XMPP</td>
<td>5222</td>
</tr>
</tbody>
</table>

Task 4: Validate the configuration
1 Launch the RealPresence Mobile application from a public network.
2 Make sure that the mobile device is connected to a 3G/4G or WiFi network outside the corporate network, and that there is no VPN client running on the mobile device.
3 Sign in using username@example.com with the correct credentials.
   After RealPresence has signed in and obtained provisioning information, it registers to the gatekeeper using the VBP-ST’s public IP address.
4 Search for a user from the directory.
5 Place a point-to-point call to the user.

Configuring the RMX System

Deploy the RMX system to provide audio/video conference service for endpoints.

The following configuration is needed for the RMX system to support the CMA system as H.323 gatekeeper deployment. Polycom recommends that you enable Siren™ Lost Packet Recovery (LPR) on the RMX system.
Task Overview

1. Configure CMA system as primary gatekeeper for the RMX system.
2. Ensure that Polycom Siren LPR is enabled.

Task 1: Configure CMA system as primary gatekeeper for the RMX system

1. On the RMX Management pane, click IP Network Services.
2. On the Network list pane, double-click Default IP Service to open the Default IP Service Properties dialog box.
3. Click the Gatekeeper tab.
   a. Select H.323 or H.323&SIP for IP Network Type.
   b. Specify the gatekeeper address.
   c. Enter the FQDN of the CMA system as the Primary Gatekeeper. For example, enter cma.example.com.
   d. Enter the dialing prefix for MCU Prefix in Gatekeeper.
   e. Add Alias for this RMX system.

Task 2: Ensure that Polycom Siren LPR is enabled

Siren LPR helps to ensure good audio quality. By default, Siren LPR is enabled. To determine its status, verify the value of the system flag ENABLE_SIRENLPR.

1. On the RMX Management pane, go to Setup/System Configuration.
2. Search for the flag name ENABLE_SIRENLPR.
   - If no flag is found, the default value is YES and Siren LPR is enabled.
   - If its value is NO, change the value to YES.

You can create meeting rooms or enable ad-hoc meetings to enable Polycom RealPresence Mobile to join a conference. For more information about the conference service and other features provided by RMX systems, refer to the Polycom RMX 1500/2000/4000 Administrator’s Guide, available at support.polycom.com.

Configuring the RealPresence Mobile Systems

Polycom RealPresence Mobile is supported for use on Apple iPad2, Apple iPhone 4S, Motorola XOOM, Motorola DROID XYBOARD, and Samsung Galaxy Tab. This section serves as a reference to help end users configure RealPresence Mobile systems in the most convenient way.

For detailed configuration steps and a feature list, refer to Help. Refer also to the appropriate version of Release Notes for the software version you are using, available at support.polycom.com.
Individual end users should request help from their organization’s IT department. IT professionals can get assistance in Polycom’s Support Community (forum) at community.polycom.com.

**Task Overview**

1. Install or upgrade RealPresence Mobile.
2. Configure Sign-In settings.
   a. Configure to register to a provisioning server. (Recommended)
   b. Configure for use without registering to a provisioning server.
3. (Optional) Configure Network Settings.

**Task 1: Install or upgrade RealPresence Mobile**

Use the same procedures for installing and upgrading RealPresence Mobile on iOS and Android devices as you use for installing and upgrading other iOS and Android applications.

When you visit Google Play or the Apple® App Store, search for ‘polycom’ or ‘video conferencing’ to find the RealPresence Mobile application.

When you uninstall the application, your user data is deleted.

**Task 2: Configure Sign-In settings**

Users can choose to configure RealPresence Mobile to register to a provisioning server. Registering to a provisioning server is recommended to enable easy setup and access to advanced features.

Sign in to the provisioning server with the user name and password. The account can be created locally on the provisioning server or integrated into the provisioning server from enterprise Active Directory server.

**Configure to Register to a Provisioning Server (Recommended)**

When users set up the system for the first time, they can configure the system to find the provisioning server in either of the following ways:

- Discover the provisioning server address automatically.

  When users choose to find the provisioning server automatically, the RealPresence Mobile system uses the email address to find the provisioning server by using a DNS SRV query.
For example, if you enter the Email Address as username@example.com and DNS service has been correctly configured, RealPresence Mobile systems automatically finds the IP address of the provisioning server in domain example.com.

- Specify the provisioning server address manually.

If the DNS service is not available, users can enter the provisioning server address information manually. The system then registers to the provisioning server each time the user signs in.

- For the iPhone 4S, users can leave the email address field empty, and then click Next to enter the server address.
- For iPad2 and Android tablets, users can enter any information in the email address field, and then go to Settings to enter the server address manually.

Configure for Use without Registering to a Provisioning Server (Not Recommended)

On iPad2 and Android tablets, users can use RealPresence Mobile without registering to a provisioning server. This type of operation is not recommended because the user is unable to use advanced features, such as sending and receiving content and LDAP search. In addition, the user must configure all settings manually.

For more details, refer to Help. Refer also to the Release Notes for the software version you deploy, available at support.polycom.com.

Task 3: (Optional) Configure Network Settings

You can configure the following parameters in Network Settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN Call Rate</td>
<td>Specifies call rate to use for calls using a wireless LAN.</td>
</tr>
<tr>
<td>3G/4G Call Rate</td>
<td>Specifies the call rate to use for calls using a 3G or 4G Network.</td>
</tr>
</tbody>
</table>

If Automatic Provisioning Profile has been configured on the CMA server and Maximum Speed for Receiving Calls (Kbps) and Preferred Speed for Placing Calls (Kbps) are set to different values from the Network Settings on RealPresence Mobile, RealPresence Mobile uses the lower values while placing or receiving calls.
Polycom DMA System as H.323 Gatekeeper

In this deployment model, the Polycom CMA system functions as the provisioning server. The Polycom DMA system functions as the gatekeeper.

**Deployment Model Advantages**

The Polycom DMA system can act as the H.323 Gatekeeper. A single DMA system can support up to 15,000 device registrations and up to 5,000 audio/video concurrent calls. In this deployment model, the Polycom CMA system functions as the provisioning server to the Polycom RealPresence Mobile system.
Deployment Architecture

The following figure illustrates the reference architecture for this deployment model.
### Function Description

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and Provisioning</td>
<td>The Polycom CMA system provides authentication and provisioning services to the Polycom RealPresence Mobile system. Authentication can be performed by the CMA system locally or through the organization's Active Directory server.</td>
</tr>
<tr>
<td>Directory</td>
<td>The CMA system provides global directory service to the RealPresence Mobile system through either the local directory or the organization's Active Directory server.</td>
</tr>
<tr>
<td>Device Management</td>
<td>The CMA system can perform limited monitoring of the RealPresence Mobile systems, such as online, offline, and in-call, but it does not support automatic software updates for RealPresence Mobile systems. The DMA system can provide call reports, such as Call Detail Records reports.</td>
</tr>
<tr>
<td>Registration and Call Control</td>
<td>H.323 registration and call control services are provided by the DMA system.</td>
</tr>
<tr>
<td>Access from an External Network</td>
<td>The Polycom VBP-ST system provides the firewall traversal service when RealPresence Mobile systems access the CMA and DMA system from an external network (Internet). If there is an existing VPN deployment for Internet access, RealPresence Mobile systems can access the CMA and DMA systems through VPN connect.</td>
</tr>
<tr>
<td>Video Conference</td>
<td>The Polycom RMX system provides audio and video conference service for RealPresence Mobile. You can configure the Polycom DMA system to manage RMX systems.</td>
</tr>
<tr>
<td>Split DNS</td>
<td>Split DNS enables RealPresence Mobile systems to use the identical SRV records or FQDNs from both internal and external network (Internet).</td>
</tr>
<tr>
<td>DNS Load Balancing</td>
<td>Deploying more than one VBP-ST system can provide load balancing through DNS configuration when RealPresence Mobile systems access from an external network (Internet).</td>
</tr>
</tbody>
</table>

### Device Licensing

#### CMA Seat Licenses for RealPresence Mobile

Refer to the CMA Seat Licenses rules described in the section CMA Seat Licenses for RealPresence Mobile. Both deployment models follow the same rules.
DMA Licenses for RealPresence Mobile

DMA licenses only limit the number of concurrent calls. For example, if the DMA licenses number is 100, up to 100 concurrent calls are allowed for all endpoints registering to this DMA system.

Solution Overview

The following tasks are required for deploying RealPresence Mobile in an environment that uses DMA as H.323 gatekeeper.

1. Configuring the DNS service.
2. Configuring the CMA system.
3. Configuring the DMA system.
4. Configuring the VBP-ST system.
5. Configuring the RMX system.
6. Configuring the RealPresence Mobile systems.

Configuring the DNS Service

For configuring the DNS service, refer to Configuring the DNS Service. For DNS configuration, the procedures are the same.

Polycom does not provide support for setting up or configuring the DNS service.

Configuring the CMA System

The tasks for configuring the CMA system are similar to those described in the deployment model Polycom CMA System as H.323 Gatekeeper. The following information describes differences in the configuration procedures.

The first task for configuring the CMA system described in the deployment model Polycom CMA System as H.323 Gatekeeper does not apply in the deployment model that uses DMA as H.323 gatekeeper.

In the DMA system as H.323 gatekeeper model, CMA is not needed as H.323 gatekeeper.
**Task Overview**

1. Edit site topology.
2. Create user accounts for RealPresence Mobile.
3. Set up provisioning for RealPresence Mobile.

**Task 1: Edit site topology**

Refer to Task 2: Edit site topology.

**Task 2: Create user accounts for RealPresence Mobile**

Refer to Task 3: Create user accounts for RealPresence Mobile.

**Task 3: Set up provisioning for RealPresence Mobile**

Provisioning information for RealPresence Mobile is configured from two places on CMA. The site provisioning covers H.323, security, and firewall settings. Automatic provisioning covers settings of **Maximum Speed for Receiving Calls (Kbps)** and **Preferred Speed for Placing Calls (Kbps)**.

1. Configure site provisioning for a site that does not include your VBP-ST.
   a. Go to Admin > Dial Plan and Sites > Sites.
   b. In the Site list, select the site that includes the RealPresence system, and select **Edit Site Provisioning Details**.
   c. In the H.323 Settings pane, select **Enable IP H.323**, and specify the IP address of the DMA system for the **Gatekeeper IP Address** field.
   d. In the Security Settings pane, select **When Available** for AES Encryption.
   e. Edit other site provisioning settings as needed, and click **OK**.

2. Configure site provisioning for a site that includes your VBP-ST system exclusively.
   a. Go to Admin > Dial Plan and Sites > Sites.
   b. In the Site list, select the site that includes the RealPresence system, and then select **Edit Site Provisioning Details**.
In the H.323 Settings pane, select **Enable IP H.323**, and then select **This Server**.

Ensure that **Enable H.460 Firewall Traversal** is enabled in Firewall Settings.

In the Security Settings pane, select **When Available** for AES Encryption.

Edit other site provisioning such as security, and click **OK**.

Configure automatic provisioning.

Refer to the steps described in **Task 4: Set up provisioning for RealPresence Mobile**.

### Configuring the DMA System

In this deployment model, the DMA system serves as H.323 gatekeeper.

The following deployment procedure includes only those steps necessary to enable RealPresence Mobile usage. For details about other features provided by the DMA system, such as MCU resource management, refer to the *Polycom DMA7000 System Version 4.0 Operations Guide*, available at [support.polycom.com](http://support.polycom.com).

### Task Overview

1. Enable H.323 signaling and set Gatekeeper call mode.
2. (Optional) Create the site topology.

#### Task 1: Enable H.323 signaling and set Gatekeeper call mode

1. Log into the Polycom DMA system.
2. Go to **Admin > Local Cluster > Signaling Settings**.
3. Enable the **Enable H.323 signaling** setting, and click **Update**.
4. Go to **Admin > Call Server > Call Server Settings**.
5. Select **Routed call mode** as **Gatekeeper call mode**, and click **Update**.
**Task 2: (Optional) Create the site topology**

For a large enterprise that includes multiple branches and complex network deployment, site topology is recommended for bandwidth management and registration control.

For simple network topology or a limited numbers of users, creating the site topology is optional.

**To Create the Site Topology:**

1. Log into the Polycom DMA system.
2. Go to **Network > Site Topology > Sites**.
3. For each site, click Add, and create a new site by entering the following information:
   - **Site Name**: Name of the site, for example, sitea, site_VBP, siteb.
   - **IP Range**: IP addresses used for the RMX, VBP, and clients in the site.
4. Configure the network clouds.
   - Go to **Network > Site Topology > Network Clouds**.
   - Click Add, and create a Network Cloud/Backbone.
   - Associate the Network Cloud/Backbone with a site, for example, sitea.
   - Click Add Site Links to set up site links between the site and the Network Cloud.
   - Repeat steps a through d for each site.
5. Create site links from the sites to the Internet.
   - Go to **Network > Site Topology > Site Links**.
   - Click Add Site Links to set up links from each site to the Internet.
6. Configure territories.
   - Go to **Network > Site Topology > Territories**.
   - Click Add, and configure each territory with Name and Description.
   - For each territory, configure the primary node as the DMA cluster.
   - Associate each territory with its corresponding sites. For example, associate Territory1 with sitea and associate Territory2 with site_VBP.

**Configuring the VBP-ST System**

VBP-ST system configurations for the deployment model using DMA as H.323 gatekeeper are similar to those in the deployment model using CMA as H.323 gatekeeper.
The following information describes differences in the configuration procedures.

**Task Overview**

1. Configure VBP-ST network settings.
2. Configure the CMA system to collaborate with VBP-ST.
3. Configure DMA to collaborate with VBP-ST.
4. Configure the VBP-ST system to collaborate with CMA and DMA.
5. Validate the configuration.

**Task 1: Configure VBP-ST network settings**
Refer to Task 1: Configure VBP-ST network settings.

**Task 2: Configure the CMA system to collaborate with VBP-ST**
Refer to Task 2: Configure CMA system to collaborate with VBP-ST.

- Polycom recommends that you add the VBP-ST system to a unique site that includes only the VBP-ST system without any endpoints.

**Task 3: Configure the DMA system to collaborate with VBP-ST**
If you configure sites on the DMA system, you should also add VBP-ST to a site by specifying the subnet or IP address of the VBP-ST’s Provider Interface.

Refer to Task 2: (Optional) Create the site topology.

**Task 4: Configure the VBP-ST system to collaborate with CMA and DMA**
Refer to Task 3: Configure VBP-ST system to collaborate with CMA.

- When you configure the VBP-ST VoIP ALG H.323 settings, enter the IP address of the DMA system as the **WAN/Provider-side GK address**.

**Task 5: Validate the configuration**
Refer to Task 4: Validate the configuration.
Configuring the RMX System

The RMX system is deployed to provide audio and video conference service for endpoints. For basic information, refer to Configuring the RMX System.

For the primary gatekeeper, configure the DMA system instead of the CMA system.

For information on using the DMA system to manage MCU resources, refer to the Polycom RMX 1500/2000/4000 Administrator’s Guide, available at support.polycom.com.

Configuring the RealPresence Mobile Systems

Refer to Configuring the RealPresence Mobile Systems. For RealPresence Mobile system configuration in both deployment models, the procedures are the same.
This chapter describes how to plan for the number of users and the amount of server load required for the UC Infrastructure.

**RealPresence Mobile User Models**

RealPresence Mobile users can join a conference from most WiFi, 3G, or 4G networks. On a corporate WiFi network, RealPresence Mobile calls originate within the corporate network. Otherwise, the traffic must pass through the Polycom VBP-ST.

Supported call rates for RealPresence Mobile depend on the type of video codec used by the device, as shown in the following table.

<table>
<thead>
<tr>
<th>Codec Type</th>
<th>Devices</th>
<th>Max Call Rate, Resolution</th>
<th>Default Call Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware-based</td>
<td>Motorola Xoom</td>
<td>1920 kbps, 720p</td>
<td>512 kbps (WiFi) 256 kbps (3G/4G)</td>
</tr>
<tr>
<td></td>
<td>Samsung Galaxy Tab 10.1&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software-based</td>
<td>Motorola Xyboard</td>
<td>512 kbps, QVGA (320 x 240)</td>
<td>512 kbps (WiFi) 256 kbps (3G/4G)</td>
</tr>
<tr>
<td></td>
<td>Samsung Galaxy Tab (Qualcomm based)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iPad2</td>
<td>512 kbps, (480 x 352)</td>
<td>512 kbps (WiFi) 256 kbps (3G)</td>
</tr>
<tr>
<td></td>
<td>iPhone4S</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Considering packet overhead, the actual bandwidth consumption of one user is shown in the following table.

<table>
<thead>
<tr>
<th>Call Rate</th>
<th>Overhead</th>
<th>Bandwidth Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>512 kbps</td>
<td>25%</td>
<td>640 kbps</td>
</tr>
<tr>
<td>1920 kbps</td>
<td>25%</td>
<td>2400 kbps</td>
</tr>
</tbody>
</table>
To facilitate capacity calculation, the following are assumed.

<table>
<thead>
<tr>
<th>Call Origin</th>
<th>Bandwidth</th>
<th>Typical Corporate Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet via VBP-ST</td>
<td>640 kbps, CIF resolution</td>
<td>20%</td>
</tr>
<tr>
<td>Corporate network</td>
<td>640 kbps, CIF resolution</td>
<td>80%</td>
</tr>
<tr>
<td></td>
<td>2400 kbps, 720p resolution</td>
<td></td>
</tr>
</tbody>
</table>

In addition, assume that up to 20% of total users are in a video call at the same time.

When planning the deployment and calculating how many servers are required, you should evaluate whether these assumptions are correct for your production network.

**Estimating Server Capacity**

The CMA server is used for device management and provisioning. The CMA 4000 system supports up to 400 users. The CMA 5000 system supports up to 5000 users.

The DMA system is used in an environment that requires RMX Resource Management and the H.323 Gatekeeper with a larger capacity.

VBP-ST series systems are used for firewall traversal. The VBP 5300-ST system supports up to 100 registered users and 25 Mbps of traffic. The VBP 6400-ST system supports up to 250 registered users and 200 Mbps of traffic.

While designing the deployment strategy, consider the capacity of all types of servers to ensure end-to-end support to an estimated number of users.

The following table describes the capabilities of Polycom servers.

<table>
<thead>
<tr>
<th>Server</th>
<th>Capacity per unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMA 7000</td>
<td>15,000 device registrations</td>
</tr>
<tr>
<td></td>
<td>5,000 audio/video concurrent calls</td>
</tr>
<tr>
<td></td>
<td>64 Polycom RMX 1500/2000/4000</td>
</tr>
<tr>
<td>CMA 5000</td>
<td>5,000 users:</td>
</tr>
<tr>
<td></td>
<td>• 1500 concurrent calls in Routed Mode</td>
</tr>
<tr>
<td></td>
<td>• 3000 calls in Direct Mode</td>
</tr>
<tr>
<td>CMA 4000</td>
<td>400 users:</td>
</tr>
<tr>
<td></td>
<td>• 120 concurrent calls in Routed Mode</td>
</tr>
<tr>
<td></td>
<td>• 240 calls in Direct Mode</td>
</tr>
</tbody>
</table>
Before you begin to calculate capacity, supply the information required in this worksheet.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;#User&gt;</td>
<td>Number of RealPresence Mobile users</td>
</tr>
<tr>
<td>&lt;#Call&gt;</td>
<td>Number of active calls at any one time. Typically, this is 20% of &lt;#User&gt;.</td>
</tr>
<tr>
<td>&lt;#ExtUser&gt;</td>
<td>Number of RealPresence Mobile users through VBP-ST. Typically, this is 20% of &lt;#User&gt;.</td>
</tr>
<tr>
<td>&lt;#ExtCall&gt;</td>
<td>Number of calls originating through VBP-ST. Typically, this is 20% of &lt;#ExtUser&gt;.</td>
</tr>
<tr>
<td>&lt;#P2PCall&gt;</td>
<td>Number of users in Point-to-Point calls at any one time. Typically, this is 40% of &lt;#Call&gt;.</td>
</tr>
</tbody>
</table>
### Formulas

The following table shows how to calculate the required number of each type of servers.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;#MPCall&gt;</td>
<td>Number of users in Multi-Point calls at any one time. Typically, this is 60% of &lt;#Call&gt;.</td>
</tr>
<tr>
<td>&lt;BW&gt;</td>
<td>Bandwidth of calls placed from corporate network.</td>
</tr>
<tr>
<td>&lt;ExtBW&gt;</td>
<td>Bandwidth of calls placed from Internet via VBPST.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMA 4000</td>
<td>&lt;#User&gt; up to 400 users</td>
</tr>
<tr>
<td>CMA 5000</td>
<td>&lt;#User&gt; up to 5,000 users</td>
</tr>
<tr>
<td>DMA 7000 as H.323 Gatekeeper</td>
<td>Up to 15,000 device registrations&lt;br&gt;Up to 5,000 audio/video concurrent calls</td>
</tr>
<tr>
<td>RMX 4000</td>
<td>CIF Resolution: &lt;#MPCall&gt; / 360&lt;br&gt;720p Resolution: &lt;#MPCall&gt; / 120</td>
</tr>
<tr>
<td>RMX 2000</td>
<td>CIF Resolution: &lt;#MPCall&gt; / 180&lt;br&gt;720p Resolution: &lt;#MPCall&gt; / 60</td>
</tr>
<tr>
<td>RMX 1500</td>
<td>CIF Resolution: &lt;#MPCall&gt; / 90&lt;br&gt;720p Resolution: &lt;#MPCall&gt; / 30</td>
</tr>
<tr>
<td>VBP 6400-ST</td>
<td>Choose the larger of the following:&lt;br&gt;&lt;#ExtUser&gt; / 250&lt;br&gt;&lt;#ExtCall&gt; * &lt;ExtBW&gt; / 200Mbps</td>
</tr>
<tr>
<td>VBP 5300-ST</td>
<td>Choose the larger of the following:&lt;br&gt;&lt;#ExtUser&gt; / 100&lt;br&gt;&lt;#ExtCall&gt; * &lt;ExtBW&gt; / 25Mbps</td>
</tr>
</tbody>
</table>
The following table shows the number of servers needed in an environment with 5000 registered users, using CMA as the H.323 gatekeeper.

<table>
<thead>
<tr>
<th>Server</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variables</td>
<td>&lt;#User&gt;5000</td>
</tr>
<tr>
<td></td>
<td>&lt;#Call&gt;1000</td>
</tr>
<tr>
<td></td>
<td>&lt;#ExtUser&gt;1000</td>
</tr>
<tr>
<td></td>
<td>&lt;#ExtCall&gt;200</td>
</tr>
<tr>
<td></td>
<td>&lt;#MPCall&gt;600</td>
</tr>
<tr>
<td></td>
<td>&lt;ExtBW&gt;640 Kbps</td>
</tr>
<tr>
<td>CMA 5000</td>
<td>1</td>
</tr>
<tr>
<td>RMX 4000</td>
<td>CIF Resolution: 2</td>
</tr>
<tr>
<td></td>
<td>720p Resolution: 5</td>
</tr>
<tr>
<td>VBP 6400-ST</td>
<td>4</td>
</tr>
</tbody>
</table>