Deploying Polycom® Unified Communications in an Acme Packet® Net-Net Enterprise Session Director Environment
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 property of their respective owners.
About This Guide

Deploying Polycom Unified Communications in an Acme Packet Net-Net Enterprise Session Director Environment includes requirements for Polycom and Acme Packet Net-Net Enterprise Session Director (ESD) interoperability.

It describes how to enable Polycom products to provide firewall traversal for required connections using the Acme Packet Net-Net Session Border Control (SBC). It also describes how remote clients are provisioned and managed within the Acme Packet Net-Net SBC Environment.

This guide describes how to deploy the solution in a corporate SIP environment. It does not discuss considerations for deploying Polycom or Acme Packet products in H.323 environments.

Related Documentation

Please refer to the product documentation for the appropriate Polycom product for detailed documentation. You can find Polycom product documentation online at http://support.polycom.com.

For detailed information about Acme Packet Net-Net ESD, refer to Acme Packet documentation online at https://support.acmepacket.com/documentation.asp.

Required Skills

Integrating Polycom infrastructure and endpoint systems with the Acme Packet Net-Net ESD requires planning and elementary knowledge of Polycom video conferencing and video conferencing administration.

Polycom assumes the readers of this guide have a basic understanding of SIP, Acme Packet and Polycom device concepts. Users should also be comfortable with navigating and configuring Acme Packet Net-Net ESD.

Users should have knowledge of Microsoft® Windows Exchange Server 2010.
Polycom Solution and Support Services

Polycom Implementation and Maintenance services provide support for Polycom solution components only. For Acme Packet Net-Net Enterprise Session Director issues, contact your Acme Packet support representative.

Please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative for more information.
Contents

Related Documentation ................................................................. iii
Required Skills ........................................................................... iii
Polycom Solution and Support Services ........................................ iv

1 Getting Started with Acme Packet® Net-Net Enterprise Session Director ................................................................. 1
   Overview of the Acme Packet Net-Net Enterprise Session Director ........................................................................ 1
   Deploying the Acme Packet Net-Net Enterprise Session Director .......................................................................... 2

2 Polycom Unified Communications in an Acme Packet Net-Net ESD Environment ................................................. 5
   Supported Deployment Models .................................................. 6
   Remote User Collaboration in an Acme Packet Net-Net ESD Environment .......................................................... 6
   Guest User Collaboration in an Acme Packet Net-Net ESD Environment .......................................................... 6

3 Remote User Collaboration in an Acme Packet Net-Net ESD Environment ................................................................. 7
   Products Used in Testing This Solution ..................................... 7
   Deployment Architecture .......................................................... 9
   Solution Task Overview .............................................................. 9
   Configure the Acme Packet Net-Net Enterprise Session Director ........................................................................ 9
   Configure Polycom Applications and Platforms ....................... 10
   Configure Polycom Endpoints ................................................... 10
   Configure Polycom RSS Server ............................................... 12
   Configure Microsoft Exchange Server 2010 ............................. 12
   Configure DNS and Certificates ............................................... 12

4 Guest User Collaboration in an Acme Packet Net-Net ESD Environment ................................................................. 15
   Supported Products .................................................................. 15
   Deployment Architecture .......................................................... 16
   Solution Task Overview .............................................................. 17
   Configure Acme Packet Net-Net Enterprise Session Director ........................................................................ 17
   Configure Polycom Applications and Platforms ....................... 17
   Task 1: Configure DMA systems to enable SIP signalling ........... 17
   Configure Polycom Endpoints ................................................... 17
   Task 1: Configure Polycom HDX Systems ................................. 17
Deploying Polycom® Unified Communications in an Acme Packet® Net-Net Enterprise Session Director Environment

Task 2: Configure Polycom RealPresence Mobile Systems  
Configure Polycom RSS Server  
Configure DNS and Certificates  
Guest User Dial String Formats

5 Configuring Polycom Products in an Acme Packet Net-Net ESD Environment

Polycom RealPresence Resource Manager System  
Configure the RealPresence Resource Manager System in Standard Security Mode  
Configure Enterprise Directory Server Integration  
Configure Provisioning Information for Acme Packet Net-Net ESD components in the RealPresence Resource Manager system

Polycom Distributed Media Application (DMA) System  
Configure the DMA System  
Configure Device Authentication  
Create the DMA System Site Topology  
Add a Special Dial Rule  
Enable SIP Signaling

Polycom RMX Conferencing Platforms

Polycom RSS Server  
Configure Polycom RSS Server in Normal Mode

Polycom HDX systems  
Enable SIP Keep-Alive Messages  
Register HDX Systems with the RealPresence Resource Manager System Provisioning Service

Polycom RealPresence Mobile  
Configure Certificate Verification  
Register RealPresence Mobile Systems with the RealPresence Resource Manager System Provisioning Service

6 Configuring the Acme Packet Net-Net ESD

Configure the Acme Packet Net-Net ESD
Acme Packet® Net-Net Enterprise Session Director is a session border controller (SBC). A session border controller (SBC) provides critical control functions to enable high quality interactive communication — voice, video, and multimedia sessions — across IP network borders.

Acme Packet Net-Net Enterprise Session Director secures the borders to the service provider IP network, the private VPN that connects major enterprise or contact center sites, and the Internet. This allows for secure communication between remote office and remote users, as well as users and organizations outside of the enterprise.

Overview of the Acme Packet Net-Net Enterprise Session Director Solution

The Acme Packet Net-Net Enterprise Session Director solution consists of the following components:

- An Acme Packet Net-Net Enterprise Session Director media relay that enables media connections to traverse the firewall
- A signaling access component within the Acme Packet Net-Net Enterprise Session Director to provide access for signaling (SIP), presence (XMPP), directory (LDAP) and provisioning (HTTP).
Microsoft® Exchange Edge Transport Server which provides connections required for Polycom® endpoints to access calendaring.

Deploying the Acme Packet Net-Net Enterprise Session Director

There are two ways to deploy the Acme Packet Net-Net Enterprise Session Director within the solution.

In the first—and recommended—deployment architecture, the Acme Packet Net-Net Enterprise Session Director is deployed parallel to the corporate firewall as shown in the following illustration.

The advantage of this deployment architecture is that it avoids open port mismatches between the Acme Packet Net-Net Enterprise Session Director and the firewall.
In the second deployment architecture, the Acme Packet Net-Net Enterprise Session Director is deployed in the DMZ. In a DMZ configuration, the Acme Packet system runs behind the firewall. The advantage of this approach is that the security functionality in the corporate firewall can be used. The disadvantage of this approach is that all traffic (media and signaling) flows through the corporate firewall, which can affect performance.

The following figure shows the Acme Packet Net-Net Enterprise Session Director deployed in the DMZ.
Polycom Unified Communications in an Acme Packet Net-Net ESD Environment

Polycom’s integrated suite of hardware devices and software applications allows you to share high-quality video and audio communications between enterprise, enterprise remote users, and guest users in business-to-business collaboration.

Specifically, the Polycom video infrastructure allows you to integrate with Acme Packet Net-Net ESD to provide remote provisioning and management for remote clients as well as firewall traversal for all the required connections:

• SIP Signaling
• Encryption of signaling (TLS) and media (SRTP)
• Presence (XMPP) Signaling
• Audio and video media
• Far end camera control
• BFCP for content channel management
• Calendaring (Microsoft Exchange Server 2010)
• Directory (LDAP) and management
• Provisioning and remote management of clients
Supported Deployment Models

Polycom supports the following deployment models when integrating Polycom Unified Communications in an Acme Packet Net-Net ESD environment.

- “Remote User Collaboration in an Acme Packet Net-Net ESD Environment” on page 6
- “Guest User Collaboration in an Acme Packet Net-Net ESD Environment” on page 6

When deploying this solution, you must decide whether or not to enable encryption and whether or not to enable device authentication.

- Polycom recommends enabling encryption. If you enable encryption, additional setup is required. Both encryption options are documented in this guide.
- Enabling device authentication is optional. If you enable device authentication, guest user call flows are not supported. Guest users will be challenged for credentials they don't have, so their calls will fail.

Remote User Collaboration in an Acme Packet Net-Net ESD Environment

A remote user is an enterprise user with a Polycom endpoint outside of your enterprise network. This deployment model enables a remote user to connect to and call other SIP endpoints just as if the user were inside the enterprise network. Remote users can also receive calls as if they were inside the network.

The remote user has access to provisioning services, directory services, XMPP contact list and presence services, SIP calling and calendaring and scheduling services.

For deployment details, see “Remote User Collaboration in an Acme Packet Net-Net ESD Environment” on page 7.

Guest User Collaboration in an Acme Packet Net-Net ESD Environment

A guest user is a user with a Polycom endpoint who can call a user within your enterprise without being a member of your enterprise. Guest users can communicate using SIP, meaning they have video, content, and audio capabilities but do not have any common presence or directory services.

Guest users cannot receive calls from users within the enterprise network.

For deployment details, see “Guest User Collaboration in an Acme Packet Net-Net ESD Environment” on page 15.
Remote User Collaboration in an Acme Packet Net-Net ESD Environment

In this deployment model, a remote user can place calls to, and receive calls from, endpoint systems on the enterprise network. The remote user in this model has access to provisioning services, directory services, XMPP contact list and presence services, SIP calling, calendaring, and scheduling services.

Products Used in Testing This Solution

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Role in Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence® Resource Manager</td>
<td>7.0</td>
<td>Provisions and manages remote endpoints, and enables directory and presence services.</td>
</tr>
<tr>
<td>Polycom Distributed Media Application™ (DMA™) 7000</td>
<td>5.0</td>
<td>Functions as SIP proxy/registrar, SIP gateway, and bridge virtualizer.</td>
</tr>
<tr>
<td>Polycom RSS® 4000</td>
<td>8.0</td>
<td>Provides recording functionality for video, audio, and content.</td>
</tr>
<tr>
<td>Polycom RMX® 4000</td>
<td>7.7</td>
<td>Provides bridge capability for SIP conferences, including support for content over video.</td>
</tr>
<tr>
<td>Polycom HDX® systems, all models</td>
<td>3.0.5</td>
<td>Serves as video endpoint that can be deployed outside the firewall in small offices and home offices.</td>
</tr>
<tr>
<td>Polycom RealPresence® Mobile</td>
<td>1.3</td>
<td>Serves as client application for supported Apple® and Android® devices.</td>
</tr>
<tr>
<td>Acme Packet</td>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Acme Packet Net-Net Enterprise</td>
<td>6.3</td>
<td></td>
</tr>
<tr>
<td>Session Director</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**

Testing was carried out specifically with the Acme Packet Net-Net Enterprise Session Director-3820 platform running S-Cx6.3.0F2 software. However other Acme Packet E-SBCs such as Net-Net ESD-4500, Net-Net ESD-SE and Net-Net ESD-VME also run the same line of C-series software and consequently these other products can also be used in Polycom RealPresence deployment architecture.

<table>
<thead>
<tr>
<th>Microsoft</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange Server 2010</td>
<td>_______</td>
</tr>
<tr>
<td>Microsoft Edge Transport Server</td>
<td>_______</td>
</tr>
</tbody>
</table>
Deployment Architecture

Set up your network as shown in the deployment architecture:

Solution Task Overview

- “Configure the Acme Packet Net-Net Enterprise Session Director” on page 9 or page 39.
- “Configure Polycom Applications and Platforms” on page 10.
- “Configure Polycom Endpoints” on page 10.
- “Configure Polycom RSS Server” on page 12.
- “Configure DNS and Certificates” on page 12.

Configure the Acme Packet Net-Net Enterprise Session Director

Refer to “Configure the Acme Packet Net-Net ESD” on page 39.
Configure Polycom Applications and Platforms

Perform the following two tasks to configure the Polycom systems for this deployment model.

**Task 1: Configure the DMA system**

1. Configure the Polycom Distributed Media Application™ (DMA™) system. Refer to “Configure the DMA System” on page 28 for instructions.

2. Configure the DMA systems to enable SIP signaling. Refer to “Enable SIP Signaling” on page 33 for instructions.

3. (Recommended) Configure device authentication on the DMA system. Refer to “Configure Device Authentication” on page 28 for instructions.

**Task 2: Configure the RealPresence Resource Manager system to integrate with the Acme Packet Net-Net ESD**


2. Configure the RealPresence Resource Manager system to integrate with the enterprise directory server. Refer to “Configure Enterprise Directory Server Integration” on page 21 for instructions.


Configure Polycom Endpoints

You must have configured provisioning of the Acme Packet ESD on the RealPresence Resource Manager system (as described above) before configuring Polycom endpoints.
Polycom recommends dynamically provisioning endpoints using the RealPresence Resource Manager system. If you do not configure Polycom endpoints to be dynamically provisioned using the RealPresence Resource Manager system, only basic registration and calls will traverse the firewall when the correct SIP proxy and registrar settings are configured.

The following lists describe the functions that will not work on Polycom RealPresence Mobile and Polycom HDX systems if the endpoints are not configured for dynamic provisioning with the RealPresence Resource Manager system:

**Polycom RealPresence Mobile systems**
- Provisioning
- People + Content:
  --Receiving Content (P+C) (BFCP)
  --On iPad, sending PDF files as content (P+C) (BFCP)
- Encrypted media (SRTP)
- Local address book
- LDAP directory access
- TLS SIP

**Polycom HDX systems**
- Provisioning
- Automatic software updates
- LDAP directory access via the RealPresence Resource Manager system.
- Presence feature via the RealPresence Resource Manager system.

Perform the following two tasks to configure the Polycom endpoint systems.

**Task 1: Configure Polycom HDX systems**

1. Configure the user name and password for the Polycom HDX system. Verify that the user name and password you configure here has been configured in the directory.
2. Enable SIP keep-alive messages. Refer to “Enable SIP Keep-Alive Messages” on page 34 for instructions.
3. Refer to “Register HDX Systems with the RealPresence Resource Manager System Provisioning Service” on page 35 to register the HDX endpoint system with the provisioning service.

Task 2: Configure RealPresence Mobile systems


2. Configure the user name and password for the Polycom RealPresence Mobile application. Verify that the user name and password you configure here has been configured in Active Directory.

3. Refer to “Register RealPresence Mobile Systems with the RealPresence Resource Manager System Provisioning Service” on page 37 to register the RPM system with the provisioning service.


Configure Polycom RSS Server

Configure the Polycom RSS server in Normal mode. Refer to “Configure Polycom RSS Server in Normal Mode” on page 34 for more information.

Configure Microsoft Exchange Server 2010

Configure the Microsoft Exchange Server 2010. Refer to Microsoft documentation for instructions.

Configure DNS and Certificates

Perform the following four tasks to configure DNS and certificates for this model. These instructions assume that both internal and external DNS servers are already set up and configured for the corporate domain.

Task 1: Configure DNS to allow endpoints to locate the provisioning server

For Polycom endpoints to automatically locate the RealPresence Resource Manager system’s provisioning service inside or outside the network, several records must be configured on the DNS system.

1. Create a DNS SRV record on the external DNS server.

   The lookup key for this service record is _cmaconfig._tcp. The record will resemble this:

   __cmaconfig._tcp.customerdomain.com 86400 IN SRV 0 0 443 Access5.customerdomain.com

   where Access5.customerdomain.com is the fully qualified domain name (FQDN) of the RealPresence Resource Manager system.
2 Set up a split DNS configuration for both the internal and external DNS servers.

For example, the Host (A) record in the internal DNS server might look like this:

```
customerdomain.com
Access5 192.168.1.15
```

where 192.168.1.15 is the internal IP address of the server.

A Host (A) record in the external DNS system might look like this:

```
customerdomain.com
Access5 222.222.222.1
```

where 222.222.222.1 is the IP address of the public side of the Acme Packet Net-Net ESD.

**Task 2: Configure certificates to allow endpoints to use the provisioning server**

Polycom endpoints connect to the RealPresence Resource Manager system for provisioning. The RealPresence Resource Manager system must have a certificate installed that is assigned to the FQDN; for example,

```
Access5.customerdomain.com
```

All certificates described in this section must come from the same Certificate Authority (CA).

1 Install a root certificate on the RealPresence Resource Manager system.

2 Install a certificate assigned to the FQDN name on the RealPresence Resource Manager system.

3 Install a root certificate on all the Polycom endpoints using provisioning.

**Task 3: Configure certificates to enable guest endpoints to use the SIP server**

Polycom endpoints connect to the SIP server using TLS. The Acme Packet Net-Net ESD must have a certificate installed that is assigned to the FQDN; for example:

```
Access5.customerdomain.com
```

All certificates must come from the same Certificate Authority (CA).

1 Install a root certificate on the Acme Packet Net-Net ESD.

2 Install a certificate assigned to the FQDN name of the Acme Packet Net-Net ESD.

3 Install a root certificate on all the Polycom endpoints using SIP over TLS.
**Task 4: Set up DNS for SIP and Microsoft Exchange Server**

The client SIP service and client Exchange service must be provisioned with an FQDN because TLS is used for these services. If you want to use the same FQDN for internal and external clients, use the split DNS method.
Guest User Collaboration in an Acme Packet Net-Net ESD Environment

In this deployment model a guest user, who is not a member of your enterprise, can call a user or bridge within your enterprise. The two users can communicate with SIP – meaning the call can have people video, content video and audio capabilities but does not have any common XMPP or directory services.

Guest user call flows are not supported when Device Authentication is enabled on the DMA system. In that scenario, guest users will be challenged for credentials they don’t have, so their calls will fail.

Supported Products

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Role in Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom Distributed Media Application™ (DMA™) 7000</td>
<td>5.0</td>
<td>Functions as SIP proxy/registrar, SIP gateway, and bridge virtualizer.</td>
</tr>
<tr>
<td>Polycom RSS® 4000</td>
<td>8.0</td>
<td>Provides recording functionality for video, audio, and content.</td>
</tr>
<tr>
<td>Polycom RMX® 4000</td>
<td>7.7</td>
<td>Provides bridge capability for SIP conferences, including support for content over video.</td>
</tr>
<tr>
<td>Polycom HDX® systems, all models</td>
<td>3.0.5</td>
<td>Serves as video endpoint that can be deployed outside the firewall in small offices and home offices.</td>
</tr>
</tbody>
</table>
### Deployment Architecture

Set up your network as shown in the deployment architecture.

![Deployment Architecture Diagram]

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
<th>Role in Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence® Mobile</td>
<td>1.3</td>
<td>Serves as client application for supported Apple® and Android® devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acme Packet</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acme Packet Net-Net ESD</td>
<td>6.3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Microsoft</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange Server 2010</td>
<td>______</td>
</tr>
<tr>
<td>Microsoft Edge Transport Server</td>
<td>______</td>
</tr>
</tbody>
</table>
Solution Task Overview

- “Configure Acme Packet Net-Net Enterprise Session Director” on page 17 or page 39.
- “Configure Polycom Applications and Platforms” on page 17.
- “Configure Polycom Endpoints” on page 17.
- “Configure DNS and Certificates” on page 18.
- “Guest User Dial String Formats” on page 19.

Configure Acme Packet Net-Net Enterprise Session Director

Refer to “Configure the Acme Packet Net-Net ESD” on page 39 for instructions on how to configure the Acme Packet Net-Net ESD.

Configure Polycom Applications and Platforms

Perform the following task to configure the Polycom applications and platforms.

**Task 1: Configure DMA systems to enable SIP signalling.**

Refer to “Enable SIP Signaling” on page 33.

Configure Polycom Endpoints

Perform the following two tasks to configure the Polycom endpoint systems.

**Task 1: Configure Polycom HDX Systems**

Refer to “Enable SIP Keep-Alive Messages” on page 34 for instructions.

**Task 2: Configure Polycom RealPresence Mobile Systems**

Refer to “Configure Certificate Verification” on page 36 for instructions.

Configure Polycom RSS Server

Configure the Polycom RSS server in Normal mode. Refer to “Configure Polycom RSS Server in Normal Mode” on page 34 for more information.
Configure DNS and Certificates

Perform the following two tasks to configure DNS and certificates for this model.

Task 1: Configure DNS to enable endpoints to locate the SIP server

For Polycom endpoints outside your enterprise to automatically locate the SIP server using a SIP URI dialing string, several records must be configured on the DNS system.

1. Create a SIP SRV record on the external DNS server.
   
   The lookup key for this service record is  _sip._tcp. The record will resemble:

   _sips._tcp.customerdomain.com 86400 IN SRV 0 0 5061 Access5.customerdomain.com

   where Access5.customerdomain.com is the FQDN of the SIP server.

   Polycom endpoints outside the enterprise will use the SRV file to the FQDN of the SIP server.

2. Set up a split DNS configuration for both the internal and external DNS servers.

   For example, the Host (A) record in the internal DNS server might look like this:

   customerdomain.com
   Access5 222.222.222.1

   where 222.222.222.1 is the IP address of the public side of the Acme Packet Net-Net ESD.

Task 2: Configure certificates to enable guest endpoints to use the SIP server

Polycom endpoints connect to the SIP server using TLS. The Acme Packet Net-Net ESD must have a certificate installed that is assigned to the FQDN; for example:

Access5.customerdomain.com

1. Install a certificate assigned to the FQDN name on the Acme Packet Net-Net ESD.

2. Install a root certificate from the same certificate authority that issued the certificate on all the Polycom endpoints using SIP services.

Use port 5060 for SIP over unencrypted UDP/TCP. Use port 5061 for encrypted SIP over TLS.
Guest User Dial String Formats

Guests must use specific dial string formats when placing calls to video meeting rooms and SIP endpoints inside the enterprise network.

- Guest users must use the following format to place a call to a Virtual Meeting Room (VMR) already configured within your enterprise DMA system:

  `<extension>@<domain>`

  `<extension>@<ip address:port>`

  Where `ip address` is the IP Address of the Acme Packet Net-Net ESD, `extension` is the VMR number and `domain` is the FQDN or IP address of the external interface of the Acme Packet. If `port` is not specified, use 5060 or 5061, as appropriate.

Use port 5060 for SIP over unencrypted UDP/TCP. Use port 5061 for encrypted SIP over TLS.

- Guest users must use the following format to place a call to a SIP endpoint inside your enterprise:

  `<name>@<domain>`

  `<name>@<ip address:port>`

  Where `ip address` is the IP Address of the Acme Packet Net-Net ESD, `name` is the SIP user name of the internal SIP endpoint and `domain` is your enterprise domain. No directory or XMPP services are available to guest users. If `port` is not specified, use 5060 or 5061 as appropriate.
Configuring Polycom Products in an Acme Packet Net-Net ESD Environment

Polycom RealPresence Resource Manager System

Use the default installation and configuration values for the RealPresence Resource Manager system except for the tasks and values listed below.

Configure the RealPresence Resource Manager System in Standard Security Mode

If during first time setup of the RealPresence Resource Manager system you are given a Security Mode option, select Set Standard Mode.

Configure Enterprise Directory Server Integration

To integrate the RealPresence Resource Manager system with an enterprise directory server:

1. Go to Admin > Directories > Enterprise Directory.
3. 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.
As needed, configure these settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain\Enterprise Directory User ID</td>
<td>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 User ID must have read permissions so it can search the entire forest on the enterprise directory server.</td>
</tr>
<tr>
<td>Enterprise Directory User Password</td>
<td>The password for the enterprise directory user account.</td>
</tr>
<tr>
<td>Security Level</td>
<td>RealPresence Resource Manager system and the enterprise directory server. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Plain—No security on the connection.</td>
</tr>
<tr>
<td></td>
<td>• LDAPS—The connection is secured over outbound port 3269 using LDAP-S in a manner similar to https. If the “Domain Controller: LDAP Server signing requirements” setting on the Active Directory server is set to “Require Signing”, then you must use LDAPS to secure the connection.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Ignore Disabled Enterprise Directory Users</td>
<td>Check this field to have the RealPresence Resource Manager system ignore disabled enterprise users in its queries.</td>
</tr>
<tr>
<td>Enterprise Directory Exclusion Filter</td>
<td>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.</td>
</tr>
<tr>
<td>Enterprise Directory Search BaseDN</td>
<td>If necessary and you understand the filter syntax, specify the top level of the enterprise directory directory tree (referred to as the base DN) to search. Don’t edit these expressions unless you understand the filter syntax.</td>
</tr>
</tbody>
</table>
Configure Provisioning Information for Acme Packet Net-Net ESD components in the RealPresence Resource Manager system

Perform the following three tasks to configure provisioning of the Acme Packet ESD.

Task 1: Create a New Site for the Acme Packet Net-Net Session Enterprise Director

Add a site and subnet for the Acme Packet Net-Net Session Enterprise Director:

1. Go to Admin > Topology > Sites.
2. On the Sites page, click Add.
3. In the Add Site dialog box, enter a Site Name and Description for the site.
4. Complete the General Info, Routing, Subnet, and if applicable ISDN Number Assignment, sections of the Add Site dialog box. The minimum information required is Site Name, Description, Location, and Subnets.
   a. Click Subnets.
   b. Click Add and enter the Acme Packet Net-Net ESD’s internal IP address in the IP Address field.
   c. Click OK.
5. Click OK.

The new site is added to the system and the Edit Site Provisioning dialog box appears. These are the site-based parameters that the RealPresence Resource Manager system automatically provisions to endpoint systems operating in dynamic management mode.

6. As needed, edit the default site provisioning details and click OK. Refer to “Task 2: Configure Provisioning Information for Solution Services” on page 23 for more information about provisioning.

Refer to the Polycom RealPresence Resource Manager System Operations Guide for more information.

Task 2: Configure Provisioning Information for Solution Services

Add provisioning information for the following services:

- SIP
- Presence
- Calendaring
- Directory
## To configure the SIP Server and SIP URI:

1. Go to **Admin > Topology > Sites**.

2. On the **Sites** page, select the site of interest and click **Edit Site Provisioning Details**.

3. In the **Edit Site Provisioning Details** dialog box, click **SIP Settings** and select these options. (Settings not listed here are optional, based on the configuration of your systems.)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP</td>
<td>Specify whether to enable SIP calls.</td>
</tr>
<tr>
<td>Automatically Discover SIP Servers</td>
<td>The RealPresence Resource Manager system will issue a DNS query to locate the SIP server and provision that information to endpoints.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Specify the FQDN or IP address of the external interface of the Acme Packet system.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Specify the IP address or DNS name of the SIP registrar server for the network.</td>
</tr>
<tr>
<td>Backup Registrar Server</td>
<td>Specify the IP address or DNS name of a backup SIP registrar server for the network.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Indicates the protocol the system uses for SIP signaling. The SIP network infrastructure determines which protocol is required.</td>
</tr>
<tr>
<td></td>
<td>- Auto enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments.</td>
</tr>
<tr>
<td></td>
<td>- TCP provides reliable transport via TCP for SIP signaling.</td>
</tr>
<tr>
<td></td>
<td>- UDP provides best-effort transport via UDP for SIP signaling.</td>
</tr>
<tr>
<td></td>
<td>- TCP/UDP port 5060.</td>
</tr>
<tr>
<td></td>
<td>- TLS provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores</td>
</tr>
<tr>
<td></td>
<td>- TLS port 5061.</td>
</tr>
<tr>
<td>SIP Server Type</td>
<td>Choose Polycom only.</td>
</tr>
<tr>
<td>Verify Certificate</td>
<td>Enable this option when the RealPresence Resource Manager system’s certificate should be verified by the certificate authority.</td>
</tr>
</tbody>
</table>
Configuring Polycom Products in an Acme Packet Net-Net ESD Environment

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Endpoint Provisioning</td>
<td>Enable this option when the system should use the provisioning credentials for SIP authentication.</td>
</tr>
<tr>
<td>Credentials</td>
<td></td>
</tr>
<tr>
<td>Common SIP User Name</td>
<td>Specify the name to use for authentication when registering with a SIP registrar server, for example, <a href="mailto:msmith@company.com">msmith@company.com</a>. If the SIP proxy requires authentication, this field and the password cannot be blank.</td>
</tr>
<tr>
<td>Common SIP Password</td>
<td>Specify the password that authenticates the system to the registrar server.</td>
</tr>
</tbody>
</table>

4  Click OK.
5  Add the SIP URI:
   a  Go to Users and select the user you want to edit.
   b  Click Edit.
   c  Click Dial String Reservations.
   d  Select the Polycom HDX system or RealPresence Mobile client you want to provision and enter the SIP URI in the SIP URI field.
      Each device must have its own, unique URI in order to register with the DMA system.
   e  Click Apply.
   f  Click OK.

Refer to the Polycom RealPresence Resource Manager System Operations Guide for more information.

To configure the presence service:
1  Go to Admin > Topology > Sites.
2  On the Sites page, select the SBC site and click Edit Site Provisioning Details.
3 In the Edit Site Provisioning Details dialog box, click Presence Settings and select these options. (Settings not listed here are optional, based on the configuration of your systems.)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Presence Server</td>
<td>Specify whether the Acme Packet Net-Net ESD will use the RealPresence Resource Manager system as the presence server or another server.</td>
</tr>
<tr>
<td></td>
<td>• This Server — The Acme Packet Net-Net ESD will use the RealPresence Resource Manager system as its presence server.</td>
</tr>
<tr>
<td></td>
<td>• Specify — The Acme Packet Net-Net ESD will use another system as its presence server.</td>
</tr>
<tr>
<td>Presence Server</td>
<td>When Use Default Presence Server is set to Specify, enter the presence server IP address in this field.</td>
</tr>
<tr>
<td>Verify Certificate</td>
<td>Enable this option when the RealPresence Resource Manager system’s certificate should be verified by the certificate authority.</td>
</tr>
</tbody>
</table>

4 Click OK.

Refer to the Polycom RealPresence Resource Manager System Operations Guide for more information.

To configure the calendaring service:

1 Go to Admin > Topology > Sites.

2 On the Sites page, select the SBC site and click Edit Site Provisioning Details.

3 In the Edit Site Provisioning Details dialog box, click Calendaring Settings and select these options. (Settings not listed here are optional, based on the configuration of your systems.)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically Discover Exchange Server</td>
<td>Specify that the CMA system should discover the Microsoft Exchange server for the site by searching DNS records.</td>
</tr>
<tr>
<td>Specify Exchange Server</td>
<td>Specify that the CMA system should use the Microsoft Exchange server specified in the Exchange Server Address field.</td>
</tr>
<tr>
<td>Exchange Server Address</td>
<td>Specify the IP address or DNS name of the Microsoft Exchange server for the site.</td>
</tr>
</tbody>
</table>

4 Click OK.
To configure the directory service:

1 Go to Admin > Topology > Sites.

2 On the Sites page, select the SBC site and click Edit Site Provisioning Details.

3 In the Edit Site Provisioning Details dialog box, click Directory Settings and select these options. (Settings not listed here are optional, based on the configuration of your systems.)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Directory Server</td>
<td>Specify whether the Acme Packet Net-Net ESD will use the RealPresence Resource Manager system as the directory server or another server.</td>
</tr>
<tr>
<td></td>
<td>• This Server — The Acme Packet Net-Net ESD will use the RealPresence Resource Manager system as its directory server.</td>
</tr>
<tr>
<td></td>
<td>• Specify — The Acme Packet Net-Net ESD will use another system as its directory server.</td>
</tr>
<tr>
<td>Directory Server</td>
<td>When Use Default Presence Server is set to Specify, enter the directory server IP address in this field.</td>
</tr>
<tr>
<td>Verify Certificate</td>
<td>Enable this option when the RealPresence Resource Manager systems certificate should be verified by the certificate authority.</td>
</tr>
</tbody>
</table>

4 Click OK.

Refer to the Polycom RealPresence Resource Manager System Operations Guide for more information.

Task 3: Add Acme Packet Net-Net Session Enterprise Director to the Network Device List

To add an Acme Packet Net-Net ESD system:

1 Go to Network Device > SBC and click Add.

   In the Add SBC dialog box, enter values for the following fields:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the Acme Packet Net-Net ESD.</td>
</tr>
</tbody>
</table>
2  Click Add.

The SBC system appears in the Network Device list.

Refer to the Polycom RealPresence Resource Manager System Operations Guide for more information.

## Polycom Distributed Media Application (DMA) System

### Configure the DMA System

In the remote user deployment model, you must configure the DMA system to integrate with the RealPresence Resource Manager system that provisions it. Integrating with a RealPresence Resource Manager system provides the DMA system with site topology information.

### Configure Device Authentication

Device authentication enhances security by requiring devices registering with or calling the DMA system to provide credentials that the system can authenticate. In turn, the DMA system may need to authenticate itself to an external SIP peer or gatekeeper.

Enabling device authentication is optional. If you enable device authentication, guest user call flows are not supported.

All authentication configurations on the DMA system are supercluster-wide, but note that the default realm for SIP device authentication is the cluster’s FQDN, allowing each cluster in a supercluster to have its own realm for challenges.

The Device Authentication page has two tabs, Inbound Authentication and Shared Outbound Authentication. For more detailed information about configuring device authentication, see the Polycom DMA 7000 System Operations Guide.

### Setting | Description
--- | ---
Provider-side IP | The private network IP address for the Acme Packet Net-Net ESD device.
Subscriber-side IP | The public network IP address for the Acme Packet Net-Net ESD device.
To configure device authentication on the DMA system:

1. Go to Admin > Call Server > Device Authentication, Inbound Authentication tab, and select Enable SIP device authentication.

2. To enter the user name and password that devices must include in their registration and signaling requests to authenticate themselves,

   a. In the Actions list, click Add.
   b. Enter the required User Name and Password.
   c. Confirm the password and click OK.

3. Leave the other settings alone unless you know you want to configure the endpoints to use a specific realm (protection domain). To do so, complete the other following fields on the Inbound Authentication tabs.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use default realm</td>
<td>This option, the default, sets the realm for the Call Server to the cluster’s FQDN (allowing each cluster of a supercluster to have its own realm). Clear the check box to change the string in the Realm field.</td>
</tr>
<tr>
<td>Realm</td>
<td>The realm string in an authentication challenge tells the challenged device the protection domain for which it must provide credentials. Generally includes the host or domain name of the Call Server. See RFC 2617 and RFC 3261.</td>
</tr>
<tr>
<td>Enable proxy authentication</td>
<td>Configures the Call Server to respond to unauthenticated requests with 407 (Proxy Authentication Required). If turned off, the Call Server responds to unauthenticated requests with 401 (Unauthorized).</td>
</tr>
<tr>
<td>Authentication valid time (seconds)</td>
<td>Specifies the time period within which the Call Server doesn’t re-challenge a device that previously authenticated itself.</td>
</tr>
</tbody>
</table>

Notes

- The name and password for a device are whatever values the person who configured the device specified. They don't uniquely identify a specific device; multiple devices can have the same name and password.
- For endpoints being dynamically provisioned, include the Common SIP Username and Common SIP Password as entered on the provisioning server in step 3 on page 24.
4 As needed, complete the following fields of the **Shared Outbound Authentication** tabs.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use default realm</strong></td>
<td>This option, the default, sets the realm for the Call Server to the cluster’s FQDN (allowing each cluster of a supercluster to have its own realm). Clear the check box to change the string in the <strong>Realm</strong> field.</td>
</tr>
<tr>
<td><strong>Realm</strong></td>
<td>The realm string in an authentication challenge tells the challenged device the protection domain for which it must provide credentials. Generally includes the host or domain name of the Call Server. See RFC 2617 and RFC 3261.</td>
</tr>
<tr>
<td><strong>Enable proxy authentication</strong></td>
<td>Configures the Call Server to respond to unauthenticated requests with 407 (Proxy Authentication Required). If turned off, the Call Server responds to unauthenticated requests with 401 (Unauthorized).</td>
</tr>
<tr>
<td><strong>Authentication valid time (seconds)</strong></td>
<td>Specifies the time period within which the Call Server doesn’t re-challenge a device that previously authenticated itself.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Lists the devices in the system’s device authentication list. Use the <strong>Search names</strong> field and <strong>Search</strong> button above the list to narrow the list. The system finds devices whose names begin with the search string.</td>
</tr>
</tbody>
</table>

**Shared Outbound Authentication**

- (table of authentication entries) Lists the authentication credential entries defined for general use by the Call Server to authenticate its requests, showing the realm in which the entry is valid and the user name. You can add, edit, or delete credential entries. Use the **Realm** or **Name** field and **Search** button above the list to narrow the list. When choosing authentication credentials to present to an external SIP peer, the Call Server looks first for an appropriate entry specific to that SIP peer. If there is none with the correct realm, it looks at the entries listed here.
5 (Optional) If a SIP peer server is configured on the DMA system, edit its configuration (Network > External SIP Peer > Edit) and configure its Authentication settings as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• Handle authentication — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server presents its authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>• Pass authentication — When it receives a 401 response from this SIP peer, the Call Server passes it to the source of the request.</td>
</tr>
<tr>
<td>Note</td>
<td>SIP authentication requests are never passed to an H.323 endpoint (a gateway call). If the Call Server can’t provide the required credentials, the call fails.</td>
</tr>
<tr>
<td>Proxy authentication</td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• Handle proxy authentication — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server presents its authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>• Pass proxy authentication — When it receives a 407 response from this SIP peer, the Call Server passes it to the source of the request.</td>
</tr>
<tr>
<td>Note</td>
<td>Authentication requests are never passed to an H.323 endpoint (a gateway call). If the Call Server can’t provide the required credentials, the call fails.</td>
</tr>
<tr>
<td>(table of authentication entries)</td>
<td>Lists the authentication credential entries defined for use with this SIP peer, showing the realm in which the entry is valid and the user name. Click Add to add authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>When choosing authentication credentials to present to this SIP peer, the Call Server looks first at the entries listed here. If there is none with the correct realm, it looks for an appropriate entry on the Device Authentication page.</td>
</tr>
</tbody>
</table>

6 (Optional) If the external SIP peer, such as another DMA, is configured to challenge for authentication credentials (inbound) and this DMA is set to handle credential challenges instead of passing them to the endpoints, then the same authentication information must be configured on the both systems. Do this on the DMA systems as follows:

a Configure the same Shared Outbound Authentication settings (see step 1 on page 29) on both systems.
b Configure the same Authentication settings (see step 5 on page 31) on both systems.

This ensures that the authentication credentials for the Shared Outbound Authentication and the SIP peer match in this 2-tier SIP server environment with only one of them doing authentication.

Create the DMA System Site Topology

To integrate with a RealPresence Resource Manager system:

1. Go to Admin > Integrations > RealPresence Resource Manager System.
2. In the Actions list, select Join Resource Manager.
3. In the Join Resource Manager dialog box, enter the host name or IP address of the RealPresence Resource Manager system and the credentials with which to log into it. Then click OK.
4. When asked to confirm that you want to join, click Yes.

The system connects to the RealPresence Resource Manager system, establishes the integration, and obtains site topology and user-to-device association data (this may take a few minutes). A dialog box informs you when the process is complete.


6. Go to Network > Site Topology > Sites, and from there to the other site topology pages, to see the site topology information obtained from the RealPresence Resource Manager system.

7. Click OK.

Add a Special Dial Rule

If your DMA system needs to be configured with an external SIP peer or an external gatekeeper, add special dial rules.

To add a special dial rule:

1. Go to Admin > Call Server > Dial Rules.
2. Click Add.
3 On the Dial Rule pane, enter values for the following fields:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The text description displayed on the Dial Rules page.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to be performed. Select Resolve to external SIP peer.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this checkbox.</td>
</tr>
</tbody>
</table>

4 Click OK.

5 Click Add.

6 On the Dial Rule pane, enter values for the following fields:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The text description displayed on the Dial Rules page.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to be performed. Select Resolve to external gatekeeper.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select this checkbox.</td>
</tr>
</tbody>
</table>

7 Click OK.

Enable SIP Signaling

Configure the DMA system to enable SIP signaling.

To configure signaling on the DMA system

1 Go to Admin > Local Cluster > Signaling Settings.

2 To make the system accessible via SIP calls:
   - Select Enable SIP signaling.
   - If the system’s security settings permit unencrypted SIP connections, optionally select TCP or UDP/TCP from the list.
     You must have the administrator role to change security settings. Leave the default port numbers (5060 for TCP/UDP, 5061 for TLS) unless you have a good reason for changing them.

3 Click Update.

A dialog box informs you that the configuration has been updated.
4 Click OK.

See the signaling configuration section of the DMA System Operations Guide for more information.

Polycom RMX Conferencing Platforms

In general, there is no special configuration required for Polycom RMX conferencing platforms. However, if Content or FECC are required within the first 30 seconds of a call, the FW NAT Keep Alive Interval on the RMX system should be modified to a lower value. For more information, see the Polycom RMX 1500/2000/4000 Administrator’s Guide.

Polycom RSS Server

Configure Polycom RSS Server in Normal Mode

The Polycom RSS 4000 server can work in two modes: normal mode and maximum security mode.

To deploy the Polycom RSS 4000 server in an Acme Packet Net-Net ESD environment, the Polycom RSS 4000 server must be in normal mode.

See the Polycom RSS 4000 System User Guide for more information about Polycom RSS server working modes.

Polycom HDX systems

Polycom HDX systems running software version 3.0.5 or later can be deployed in a Acme Packet Net-Net ESD solution.

Enable SIP Keep-Alive Messages

To deploy Polycom HDX systems within the solution, the Enable SIP Keep-Alive setting must be enabled.

To enable the Enable SIP Keep-Alive setting:
1 In the web interface, go to Admin Settings > Network > IP Network.
2 Select the Enable SIP Keep-Alive Messages check box.
Register HDX Systems with the RealPresence Resource Manager System Provisioning Service

Register each Polycom HDX system with the RealPresence Resource Manager system provisioning service.

You can register the Polycom HDX system with the RealPresence Resource Manager system in several ways:

• If the system detects a provisioning service on the network while running the setup wizard, it prompts you to enter information for registration with the service. Similarly, if the system detects provisioning data on a USB device while the running the setup wizard, it uses that information to attempt to register with the service.

The setup wizard is available during initial setup, after a software update or system reset with system settings deleted, or after using the restore button. For information about the USB device data, or about configuring the RealPresence Resource Manager system server so that Polycom HDX systems detect and register with it, refer to the Polycom Unified Communications Deployment Guide for Microsoft Environments.

• You can enter the registration information and attempt to register in the Polycom HDX system’s Admin Settings.

To configure the provisioning service settings:

1  Do one of the following:
   – In the local interface, go to System > Admin Settings > Global Services > Provisioning Service (select if necessary).
   – In the web interface, go to Admin Settings > Global Services > Provisioning Service.

2  Configure these settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Specifies the domain for registering to the provisioning service.</td>
</tr>
<tr>
<td>User Name</td>
<td>Specifies the endpoint’s user name for registering to the provisioning service.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password that registers the system to the provisioning service.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Specifies the address of the RealPresence Resource Manager system running the provisioning service.</td>
</tr>
</tbody>
</table>
3 Select Register or Update. The system tries to register with the RealPresence Resource Manager system using NTLM authentication. Refer to the provisioning service documentation in the Polycom HDX Administrators Guide for more information.

Polycom RealPresence Mobile

Configure Certificate Verification

RealPresence Mobile systems must support non-mutual and mutual certificate validation during TLS connection establishment.

To configure certificate verification for RealPresence Mobile for Apple iOS:


2 Install the client certificate:
   a Create two files.
      – Name one file client.p12. This file is a binary format PKCS12 file that includes a self certificate and self private key.
      – Name the other file client.pwd. This file contains the private key protection password encrypted by base64.
   b Import the client.pwd and client.p12 files into the application document directory using iTunes.

To configure certificate verification for RealPresence Mobile for Android:

1 Install the root certificate of the server.
   a Copy the root certificate to the root directory of the SD card.
   b From the RealPresence Mobile for Android application, go to Settings > Security and install the certificate.

2 Install the client certificate by copying the client.p12 and client.pwd files to the RealPresence Mobile for Android polycom/certificate folder.
Register RealPresence Mobile Systems with the RealPresence Resource Manager System Provisioning Service

As part of the remote user collaboration deployment model, Polycom recommends that you configure RealPresence Mobile systems to be provisioned by RealPresence Resource Manager system. If you do not configure the RealPresence Mobile systems to be provisioned by RealPresence Resource Manager system, the following remote deployment model features will not be available to RealPresence Mobile systems:

- Provisioning
- People+Content
  -- Receiving Content (either H.239 or BFCP)
  -- On iPad, sending PDF files as content (either H.239 or BFCP)
- Encrypted media
- Local address book
- LDAP directory access
- H.460 firewall traversal support for H.323
- Network location awareness

To register the RealPresence Mobile system with the RealPresence Resource Manager system provisioning service:

1. When you launch RealPresence Mobile for the first time, you are prompted for an email, user name and password.
2. Enter your email address in the Email field.
3. In the User Name field, enter the domain and password associated with the user name; for example:
   Polycom\jsmith
4. In the Password field, enter the password associated with the user name.
5. Tap Sign In.

If DNS is configured to point to the Acme Packet Net-Net ESD external interface, the RealPresence Mobile client is automatically registered to the DMA system’s SIP server and added to the RealPresence Resource Manager system for provisioning.
Configuring the Acme Packet Net-Net ESD

This chapter provides an overview of how to configure Acme Packet Net-Net ESD to interoperate with Polycom products. For more detailed information about configuring Acme Packet Net-Net ESD, refer to the Acme Packet documentation online at https://support.acmepacket.com/documentation.asp.

Configure the Acme Packet Net-Net ESD

The following table lists the required Acme Packet SBC components and their associated configuration elements:

<table>
<thead>
<tr>
<th>Acme Packet Net-Net ESD Components</th>
<th>Configuration Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP server</td>
<td>local-policy</td>
</tr>
<tr>
<td></td>
<td>sip-interface &gt; sip-ports</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>For guest user collaboration, any combination of UDP, TCP, and TLS can be used.</td>
</tr>
<tr>
<td></td>
<td>session agent</td>
</tr>
<tr>
<td></td>
<td>sip config</td>
</tr>
<tr>
<td>Presence Server (XMPP)</td>
<td>static-flow</td>
</tr>
<tr>
<td>Directory Server (LDAP)</td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>Provisioning Server (HTTPS)</td>
<td>Remote user collaboration deployment model only.</td>
</tr>
<tr>
<td>Media-manager</td>
<td>hnt-rtcp enabled</td>
</tr>
</tbody>
</table>
1. Install the Acme Packet Net-Net ESD parallel to or in the DMZ of the Corporate Firewall. See Acme Packet documentation for installation instructions at https://support.acmepacket.com/documentation.asp.

2. Configure the Acme Packet SBC Packet static flow to forward connections to the internal presence, directory and provisioning servers. See Acme Packet documentation for configuration instructions at https://support.acmepacket.com/documentation.asp.

   Use the following port numbers:

<table>
<thead>
<tr>
<th>Acme Packet Net-Net ESD Component</th>
<th>Port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence Server (XMPP)</td>
<td>5222</td>
</tr>
<tr>
<td>Directory Server (LDAP)</td>
<td>389</td>
</tr>
<tr>
<td>Provisioning Server (HTTP)</td>
<td>443</td>
</tr>
</tbody>
</table>

3. Configure the Acme Packet Net-Net ESD SIP signaling component to accept SIP sessions through UDP, TCP or TLS as required.

4. Select the media manager configuration so that you can enable `hnt-rtcp`. The default value is disabled.

5. When deploying the SBC within the DMZ, set the 1:1 NAT mappings in your corporate firewall to map to the Acme Packet Net-Net ESD components.

6. When remote access of the management interface is required, you may need to implement host-routes on the SBC.

7. Configure the firewalls adjacent to the Acme Packet signalling interface to allow the following:

   - TCP: 5060, 5061, 443, 389, 5222
   - UDP: 5060 and all ports configured in the Acme Packet “steering pool” element.

---

**To configure the Acme Packet Net-Net ESD**

<table>
<thead>
<tr>
<th>Acme Packet Net-Net ESD Components</th>
<th>Configuration Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-agent</td>
<td>Add an entry for the DMA system, specifying it by IP address and hostname, port number, transport type, and realm-id.</td>
</tr>
<tr>
<td>OUTSIDE sip-interface</td>
<td>route-to-registrar enabled register-keep-alive set to always</td>
</tr>
<tr>
<td>Media Port Range</td>
<td>steering-pool</td>
</tr>
</tbody>
</table>