Office Communications Server Setting	Polycom HDX system setting	Office Communicator calls a Polycom HDX system	Polycom HDX system calls an Office Communicator user
Required	Off	The Polycom HDX system answers the call. The call is then disconnected by Office Communicator. The following message is displayed on the Polycom HDX system: `Far site disconnected, please wait. Call cleared.`	The Polycom HDX system disconnects the call and displays the following message: `Far Site requires Encryption, please enable encryption on your system.`
	When Available	Audio-only and video calls are encrypted.	Audio-only and video calls are encrypted. If deployment includes an RMX system, the call is disconnected.
	Required for All Calls or Required for Video Calls	Audio-only and video calls are encrypted. If deployment includes an RMX system, the call is disconnected.	Audio-only and video calls are encrypted. If deployment includes an RMX system, the call is disconnected.
Off	Off	Audio-only and video calls are unencrypted.	Audio-only and video calls are unencrypted.
	When Available	Audio-only and video calls are encrypted.	Audio-only and video calls are encrypted.
	Required for All Calls or Required for Video Calls	Polycom HDX system rejects the call.	The Polycom HDX system disconnects the call and displays the following message: `Far site does not support encryption, Encryption is required for this call.`

Task 6: Test Your Deployment

Deployment Process for Polycom RMX Systems

The RMX 2000 / 4000 can host multiple video endpoints in a single conference, as well as host multiple conferences simultaneously. For these reasons, the RMX 2000 / 4000 is configured as a gateway device rather than a single user in the Office Communications Server.

See Appendix H of the *Polycom RMX 2000/4000 Administrator's Guide* for detailed steps on how to deploy a Polycom RMX 2000 / 4000 system for use with the video conferencing solution.

Deployment Process for Polycom DMA System

Task 1: Set the Routing for the Polycom DMA 7000 System

If you're including a Polycom DMA 7000 system in this solution, perform the following procedure to enable the Polycom DMA system to receive Office Communications Server calls.

To set the Polycom DMA 7000 system as a trusted host with a static route

1. Navigate to **Start > All Programs > Administrative Tools > Office Communications Server 2007 R2** to open the Office Communications Server management console.
2. In the tree, expand **Enterprise pools**, right-click the server pool entry, and select **Properties > Front End Properties**.
3. In the **Front End Properties** dialog box, select the **Host Authorization** tab and click **Add**.

   The **Add Authorized Host** dialog box is displayed.
4. Select **FQDN** and enter the fully qualified domain name associated with the Polycom DMA 7000 system's virtual interface.

Note Always refer to the system by the fully qualified domain name of its virtual interface. The system's IP addresses should be available only on the DNS server.

5. Select the **Throttle As Server** and **Treat As Authenticated** check boxes. Then click **OK**.
6. In the **Front End Properties** dialog box, select the **Routing** tab and click **Add**.

   The **Add Static Route** dialog box appears.
7. In the **Domain** field, enter the fully qualified domain name to use for the Polycom DMA 7000 system.
8. To use encrypted SIP signaling, set Transport field to **TLS**. Then click **OK**.

Note If you enable TLS security, you must also install a security certificate on the Polycom DMA 7000 system and configure the system to use TLS. See "Create a Security Certificate for the Polycom DMA 7000 System" on page 39.

In addition, you should install security certificates on your Polycom RMX MCUs and configure them to use TLS. See Appendix H of the *Polycom RMX 2000/4000 Administrator's Guide*.

The Polycom DMA 7000 system is now set as a trusted host, and calls from an Office Communicator client to a SIP address in the Polycom DMA system's domain will be routed through that system.

Task 2: Create a Security Certificate for the Polycom DMA 7000 System

If your solution includes a Polycom DMA 7000 system and you elected to use TLS transport, you must install a security certificate on the Polycom DMA 7000 system so that Office Communications Server trusts it. This can be accomplished in two ways:

- Purchase and install a certificate from a commercial Trusted Root Certificate Authority (CA) such as VeriSign or Thawte. Use the procedures in the Polycom DMA system's online help for Certificate Management to create a Certificate Signing Request and to install the certificate(s) received from the CA.
- Request and obtain a certificate from your enterprise CA. You can do this in two ways:
  - If your organization permits the submission of certificate requests directly to the enterprise's CA server, use the Office Communications Server Certificate Wizard. From it, you can then download an export file of the certificate to your PC for later installation on the Polycom DMA system. This procedure is described below.
  - If certificate requests must be submitted through the enterprise's CA team or group, use the procedures in the Polycom DMA system's online help for Certificate Management to create a Certificate Signing Request and to install the certificate(s) received from the CA team or group.

Note

Before you proceed, make certain that:

- You have all the fully qualified domain names (FQDNs) of the system for which you're creating a certificate. A two-node system has three: one virtual and two physical; a single-node system has two: one virtual and one physical.
- These host names are in the primary DNS server of the environment and resolve correctly to the Polycom DMA system.

If the host information in DNS is wrong, the certificates will not work.

To request a security certificate for the Polycom DMA system in Office Communications Server

1. Navigate to **Start > All Programs > Administrative Tools > Office Communications Server 2007 R2** to open the Office Communications Server management console.

2. In the tree, expand **Enterprise pools** and the server pools list, right-click the pool front end entry, and select **Certificate**.

   The Office Communications Server Certificate Wizard appears.

3. Follow the steps in the wizard, making the following choices:

   a. Select **Send request immediately to an online certification authority**.

   b. Select **Mark cert as exportable**.

   c. Set **Subject** name to the fully-qualified domain name (FQDN) of the Polycom DMA system's virtual interface.

   d. Enter the FQDN(s) of the physical interface(s) in the **Alternate name** field.

   e. Select a certificate authority from the list, choosing the local Office Communications Server front end entity.

   f. Skip assignment, selecting **Assign certificate later**.

   g. When done, click **Finished** to close the Wizard.

To export the received security certificate from Office Communications Server to your computer

1. In the Office Communications Server tree, expand **Enterprise pools** and the server pools list, right-click the pool front end entry, and select **Certificate**.

   The **Office Communications Server Certificate Wizard** appears.

2. Follow the steps in the wizard, making the following choices:

   a. Select **Export a certificate to a *.pfx file**.

   b. Select the certificate you created for the Polycom DMA system.

   c. Specify a path and name for the `*.pfx` file on your computer and select **Include all certificates in the certification path if possible**.

   d. Enter a password. Be sure to record what it is.

   e. Click **Finished** to download the file and close the wizard.

Once the `*.pfx` file is on your PC, you can upload it to the Polycom DMA system and install it, using the procedures in the Polycom DMA system's online help for Certificate Management.

Set Up Numerical Dialing to Virtual Meeting Rooms

When you enable numerical dialing for a virtual meeting room (VMR) on an RMX or DMA, you:

- Enable HDX or Office Communicator users to dial a number to call into a meeting room rather than a full SIP URI. This greatly simplifies dialing, especially with the HDX remote.
- Enable a common dialing plan for VMRs across Office Communications Server and H.323 infrastructures. This means that a single number can be inserted into a calendar invitation and it will be valid for Office Communications Server endpoints and H.323 endpoints.

Perform the following steps to set up numerical dialing into VMRs in the Office Communications Server infrastructure:

- "Configure the RMX/DMA as a Routable Gateway" on page 41
- "Configure an Office Communications Server Voice Route to the RMX/DMA" on page 42
- "Configure Office Communicator Users for Enterprise Voice" on page 43

You can remove numerical dialing capability at any time and return to enabling Office Communicator or HDX users to dial to meeting rooms using a matching URI, see "To Remove Numeric Dialing Capability" on page 44.

Configure the RMX/DMA as a Routable Gateway

The RMX system (or the DMA system) must be set as a routable voice gateway in the Office Communications Server infrastructure. This does not restrict the RMX system to just voice operation, rather it means that the RMX system or the DMA system can be set as a destination for a voice route in the Office Communications Server infrastructure.

The Office Communications Server infrastructure uses the WMI class `MSFT_SIPTrustedAddInServiceSetting` to store information for each voice gateway in the infrastructure. Typically, these gateways are Office Communications Server Mediation Servers, but in this case, the RMX or DMA is set as a voice gateway by creating a new instance of the class `MSFT_SIPTrustedAddInServiceSetting`.

Polycom recommends using the Office Communications Server 2007 R2 Resource Kit Tools to accomplish this.

To set up the RMX/DMA as a Voice Gateway

1. If you have not already, download and install the Office Communications Server 2007 R2 Resource Kit Tools from the following URL:

   http://www.microsoft.com/downloads/details.aspx?familyid=9E79A236-C0DF-4A72-ABA6-9A9602A93ED0&displaylang=en

2 Open a command prompt and navigate to where you installed the Office Communications Server 2007 RS resource kit. For example, `C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\`.

3 Run the following command:

```
cscript OCSTrustEntry.vbs /action:add /type:trustedservice
/fqdn:<your FQDN> /service:MediationServer /port:5061
/version:4 /routable:TRUE
```

where *<your FQDN>* is the FQDN of your RMX or DMA system.

The script automatically generates the GUID discover the proper Active Directory container to store the object.

Your RMX system (or DMA system) is now established as a trusted gateway by all Office Communications Server pools in the domain. It appears in the list of voice gateways when you establish a voice route.

4 Ensure that your DMA or RMX is not in the **Authorized Hosts** list for your Office Communications Server.

The `TrustedService` object that you just created needs to be the only trusted entry for this particular RMX/DMA. For each Office Communications Server pool, you must do the following:

a From the Office Communications Server management console, navigate to your server pool.

b Right-click the pool name and select **Front End Properties**. Then select the **Host Authorization** tab.

c Make sure the same RMX or DMA for which you created an `TrustedService` instance using the instructions above is not also in the list of authorized hosts. If it is, you MUST delete it. It is necessary to completely remove the entry from the list.

Note It may take up to five minutes for these changes to be replicated from Active Directory to the Office Communications Server repository.

Configure an Office Communications Server Voice Route to the RMX/DMA

The Voice Route to the RMX (or DMA) must be configured in the Office Communications Server.

The Office Communications Server infrastructure enables the establishment of a voice route to a voice gateway. Typically, this means that all SIP INVITEs to phone numbers which match a particular pattern will be routed to a specific gateway. In this example, all INVITEs to numbers which start with 73 will be routed to RMX210 (DNS name `rmx210.r13.vsg.local2`).

To establish a Voice Route to the RMX/DMA Voice Gateway

1. Navigate to **Start > All Programs > Administrative Tools > Office Communications Server 2007 R2** to open the Office Communications Server management console.

2. Right-click **Forest**. Then select **Properties > Voice Properties**.
3. Select the **Routes** tab in the **Office Communications Server Voice Properties** dialog.
4. Choose **Add** in the **Routes** tab.
5. Fill in the information in the **Add Route** dialog. In this example, the regex expression ^73 causes this route to be applied to all numbers starting with 73.
6. In the **Add Route** dialog, choose **Add** to set the destination gateway. The RMX gateway set up in Step 1 above, appears in the drop down list of gateways.
7. In **Phone Usages** section of the **Add Route** dialog, select a **Phone Usage** record for this route.
8. In the **Edit Route** dialog, click **OK** to save the route.
9. On the RMX which has been set up as the gateway, create meeting rooms which start with 73 (e.g., 73111). On the Office Communicator or HDX, dial 73111 and verify that the Office Communicator or HDX connects to the meeting room.

Configure Office Communicator Users for Enterprise Voice

Ensure that your Office communicator users are enabled for Enterprise Voice. You do this in the Office Communications Server management console.

To Configure Office Communicator Users for Enterprise Voice

1. Navigate to **Start > All Programs > Administrative Tools > Office Communications Server 2007 R2** to open the Office Communications Server management console.

2. Expand the Enterprise pool or Standard Edition server node where your users reside.
3. Expand the pool or server where your users reside, and then click the **Users** node.
4. In the right pane, right-click one or more users whom you want to configure, and then select **Configure users**.
5. On the **Welcome to the Configure Users Wizard** page, click **Next**.
6. On the **Configure User Settings** page, click **Next**.

7 On the **Configure Meeting Settings** page, click **Next**.

8 On the **Configure User Settings specify meeting policy** page, click **Next**.

9 On the **Configure Enterprise Voice** page, select **Change Enterprise Voice Settings for selected users**, and then click **Enable Enterprise Voice**. Click **Next**.

10 On the **Configure Enterprise Voice Settings** and **Location Profile** page, select **Change Enterprise Voice Policy for selected users**.

11 Select an Enterprise Voice policy from the list.

12 Select **Change location profile** for selected users.

13 Select a location profile from the list, and then click **Next**.

14 On the **Ready to Configure Users** page, review the settings, and then click **Next**.

15 On the **Configure Operation Status** page, verify that the operation succeeded, and then click **Finish**.

To Remove Numeric Dialing Capability

1 Remove any voice routes to the RMX/DMA which have been defined.

2 Remove the trusted service definition which you created in "To set up the RMX/DMA as a Voice Gateway" on page 41.

   a Open a command prompt and navigate to where you installed the Office Communications Server 2007 RS resource kit. For example, `C:\Program Files\Microsoft Office Communications Server 2007 R2\ResKit\`.

   b Run the following command to list each trusted service definition:

   ```
   cscript OCSTrustEntry.vbs /action:list /type:trustedservice
   ```

   An example of a returned TrustEntry is shown in Table 2-1.

Table 2-1 *Example TrustEntry*

```
 TrustEntry[6]:
CN={56A93378-FEA9-4EAE-845D-AAF0BD8073C0},CN=Trusted Services
,CN=RTC
Service,CN=Services,CN=Configuration,DC=ocs2,DC=eng,DC=westminst
er,DC=po
lycom,DC=com
        objectClass:
            top
            container
            msRTCSIP-TrustedService
        cn: {56A93378-FEA9-4EAE-845D-AAF0BD8073C0}
        distinguishedName:
CN={56A93378-FEA9-4EAE-845D-AAF0BD8073C0},CN=Trusted
Services,CN=RTC
Service,CN=Services,CN=Configuration,DC=ocs2,DC=eng,DC=westminst
er,DC=polycom,DC=com
        instanceType: 4 (0x4)
        whenCreated: 7/2/2009 8:36:57 PM
        whenChanged: 7/2/2009 8:36:57 PM
        name: {56A93378-FEA9-4EAE-845D-AAF0BD8073C0}
        objectCategory:
CN=ms-RTC-SIP-TrustedService,CN=Schema,CN=Configuration,
DC=ocs2,DC=eng,DC=westminster,DC=polycom,DC=com
        dSCorePropagationData: 1/1/1601
        msRTCSIP-TrustedServicePort: 5073 (0x13D1)
        msRTCSIP-TrustedServerFQDN:
QAOCS.ocs2.eng.westminster.polycom.com
        msRTCSIP-TrustedServiceType:
Microsoft.Rtc.Applications.Cas
        msRTCSIP-TrustedServerVersion: 4 (0x4)
        msRTCSIP-Routable: True
        msRTCSIP-ExtensionData:
TlsTarget=QAOCS.ocs2.eng.westminster.polycom.com
```

c Find the TrustEntry that includes your FQDN and use the value of the `name:` property in the next step. This is the GUID of the TrustEntry.

d Run the following command:

```
cscript OCSTrustEntry.vbs /action:remove
/type:trustedservice /CN:<GUID>
```

where `<GUID>` is the value of the `name:` property of the TrustEntry you listed in the previous step.

3 Add a Matched URI route to the RMX/DMA by right-clicking the **Office Communications Server Pool**, selecting **Properties > Front End Properties > Route**.

4 Add a host authorization for the RMX/DMA by right-clicking the **OCS Pool**, selecting **Properties > Front End Properties > Host Authorization**.

5 Wait about five minutes for Office Communicator to replicate Active Directory settings to its repository so that changes will take effect.

To Set Up Simultaneous Numerical and Matched URI Routing

You can simultaneously set up an RMX/DMA for both numerical and **Matched URI** dialing. If you want to do this, follow these instructions:

1 Set the RMX/DMA as a trusted service (MediationServer) using the instructions in "To set up the RMX/DMA as a Voice Gateway" on page 41.

2 Set up a matching URI route to the RMX/DMA by right-clicking the **OCS Pool**, selecting **Properties > Front End Properties > Routing Tab**.

3 Also set up a voice route to the same RMX/DMA using instructions in "To establish a Voice Route to the RMX/DMA Voice Gateway" on page 43.

Note

You cannot also add this DMA/RMX as an authorized host using the Front End Properties > Host Authorization tab. There can only be one trusted service entry for the RMX/DMA even though there are two different routes to the RMX/DMA (i.e., Matched URI and voice route).

Also, only TLS connections to the DMA/RMX will work, TCP connections will not work.

3

Polycom® Conferencing for Microsoft® Outlook®

Polycom Conferencing for Microsoft Outlook, which requires the Polycom Conferencing Add-in for Outlook, offers an integrated and enhanced experience for all of those involved in video conferencing.

- It allows IT departments and video administrators / operators to offer users a simple, familiar procedure for scheduling video- and audio-enabled meetings, which requires less IT support. Thus, it maximizes the use of visual communication assets and their return on investment (ROI).
- It allows conference organizers to use Microsoft Outlook and its usual meeting request workflow to schedule video- and audio-enabled meetings. It also allows conference organizers to include recording and streaming into the conference, when required.
- It allows meeting participants to track their video- and audio-enabled meetings on the same calendar that they track their other meetings. It also allows meeting participants to simply click a link in an email meeting request to join conferences on their associated video or audio endpoint system.

This chapter includes the following sections:

Polycom Products that Enable Polycom Conferencing for Outlook

System	Version	Description
Polycom HDX systems	v2.6	Monitor the Microsoft Exchange calendar of the configured account and display on-screen notifications of meetings. Users can join meetings via these notifications.
Polycom RMX 2000 or 4000 systems	v6.0	Monitors the Exchange mailbox for the Polycom Conferencing service and hosts Polycom Conferencing for Outlook conferences. Displays meeting information at the start of a meeting, called the Gathering Phase.
Polycom Conferencing Add-in for Outlook	v1.0	Allows Outlook users to schedule meetings that include video, audio, and recording. Allows invitees to join a video-enabled meeting by clicking a link.
Polycom CMA 4000 or 5000 system	v5.0	Provisions Polycom HDX systems for Polycom Conferencing for Outlook functionality and routes H.323 calls to the appropriate Polycom RMX or DMA system.
Polycom CMA Desktop	v5.0	Allows users to join video-enabled meetings by clicking a link in a meeting invitation.
Polycom DMA 7000 system	v2.0	Monitors the Exchange mailbox for the Polycom Conferencing service and determines the appropriate Polycom RMX system to host a given Polycom Conferencing for Outlook conference.
Polycom RSS 4000 system	v6.0	Via a connection from the Polycom RMX system, records Polycom Conferencing for Outlook conferences in H.323 format when selected in the Polycom Conferencing Add-in.
Polycom VBP-S/T system	v9.1.5.1	Enables H.323 Polycom HDX systems to support Polycom Conferencing for Outlook in a remote small office/home office (SOHO) network.

Microsoft Products that Enable Polycom Conferencing for Outlook

System	Version	Description
Microsoft Active Directory	2003 or 2008	Enables account logins and integrates with Microsoft Exchange. Note that Polycom products currently support only a single-forest Active Directory deployment.
Microsoft Exchange	2007 with SP1	Hosts mailboxes and calendars. SP1 is required for the 'Manage Full Access Permissions' function. Exchange Web Services must be enabled.
Microsoft Office Communications Server	2007 R2	Provides login and instant message functionality for Microsoft Office Communicator clients.
Microsoft Office Communicator	2007	Can join video-enabled meetings by clicking a link in a meeting invitation.
DNS	N/A	Permits call routing to Polycom RMX and DMA systems and DMA subscription to Exchange for mail notifications.
Microsoft Office	2007	Microsoft Outlook and Microsoft Word® 2007 are required for sending Polycom Conferencing for Outlook invitations. Users of older versions of Microsoft Office can receive invitations.

Polycom Conferencing for Outlook User Scenarios

Primary Polycom Conferencing for Outlook Scenario:

1. Organizer creates a new meeting request via his Outlook client.
2. Organizer adds meeting participants to the **To...** field in the invitation - these can be people or conference room(s). Optionally conference rooms can be added to the **Resource** field, depending on the user's preferred workflow.
3. Organizer sets the time of the meeting; this can be a specific time or a recurring meeting.
4. Organizer clicks the **Polycom** icon to make the meeting conferencing-enabled.

5 Organizer sends the meeting request.

6 Organizer receives meeting accept / reject notifications from invited participants, conference rooms and the calendaring infrastructure system.

Organizing a Polycom Conferencing for Outlook Meeting

1 Microsoft Outlook users with Exchange accounts and the Polycom Conferencing Add-in for Outlook can:

   a Use Outlook and the Conferencing Add-in to create a new Polycom conference with one or more attendees and / or conference rooms.

      In this case:

      » Conference invitees and conference rooms receive Outlook meeting requests, which they can accept or decline using standard Outlook and Exchange workflows.

      » Conference participants receive meeting reminders on their desktops via Outlook, and onscreen on both Room-based and User-based Polycom HDX systems using the Polycom Conferencing for Outlook feature.

   b Use Outlook and the Conferencing Add-in to edit or cancel a Polycom Conferencing for Outlook meeting.

      This results in a new notification being sent to participants to inform them of the revision or cancellation of the meeting. When the meeting is removed from an Exchange User or Room calendar, the HDX monitoring that account will cease to display the meeting at the next polling cycle, see “Exchange Calendar Polling Information” on page 77.

Optional Polycom Conferencing for Outlook Extensions:

1 Organizer sets an option for the meeting to be recorded. A secondary option after enabling recording is to enable streaming.

2 Organizer may update the meeting time after initial meeting creation.

3 Organizer may cancel the meeting after initial meeting creation.

4 Organizer may invite to the meeting an invitee that does not have a video device.

5 Invitee rejects the meeting request via his Outlook client.

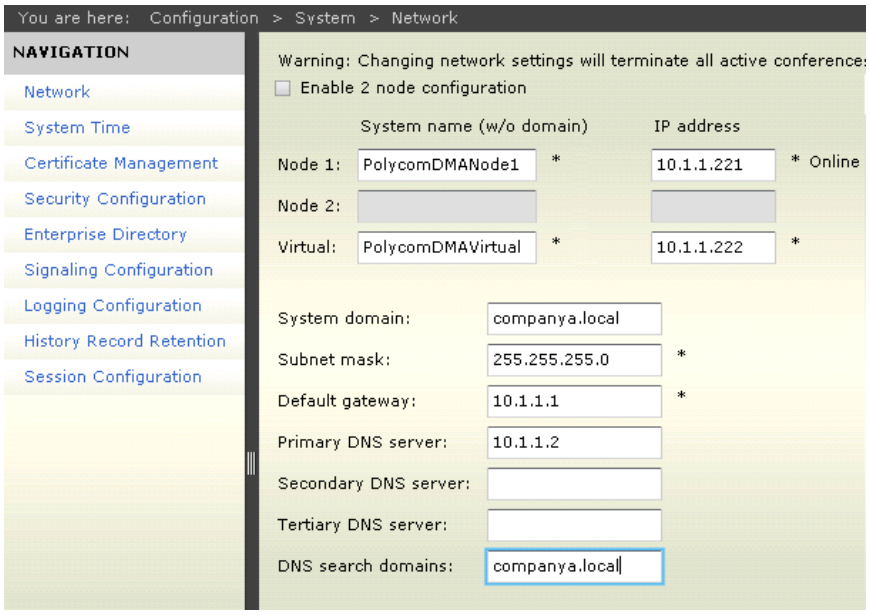
Deploying Polycom Conferencing for Outlook

Complete the following tasks to deploy Polycom Conferencing for Outlook:

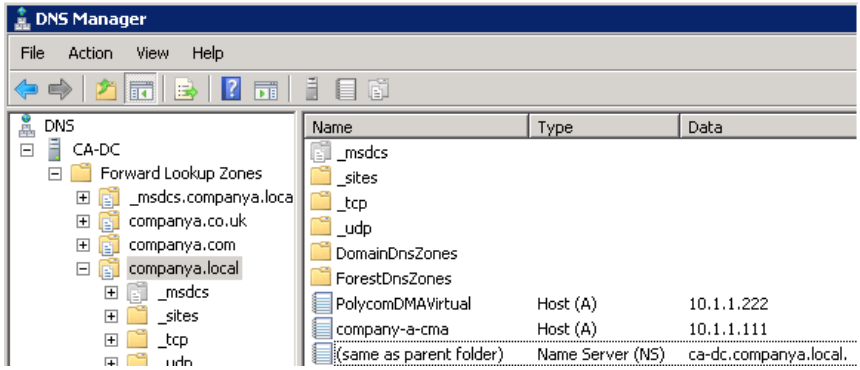
Configure DNS Entries Polycom Conferencing for Outlook

For a Polycom devices to work correctly in a Polycom Conferencing for Outlook deployment, they must subscribe to the Exchange Server for notifications when meeting invitations are sent to the Polycom Conferencing Mailbox it is monitoring. This registration will only succeed if the DNS server used by Exchange (usually, the nearest Active Directory Domain Controller provides DNS services for an Exchange Server) has an A record that resolves the Fully Qualified Domain Name of the system's Virtual IP address.

For example, Company A's DMA has a Virtual IP address of 10.1.1.222 and Virtual System name `PolycomDMAVirtual.companya.local`.



The DNS server used by Company A's Exchange Server has an A record resolving 10.1.1.222 to `PolycomDMAVirtual.companya.local`.



If the DMA system does not receive confirmation of its subscription attempt from the Exchange Server, the DMA dashboard displays 'Subscription Pending' as its Exchange integration status. This is a normal status for up to two minutes while the first-time registration process occurs. If the Exchange Server is able to resolve the DMA system's Virtual IP address as an FQDN but the DMA system still displays the 'Subscription Pending' status, there may be a firewall between DMA and the Exchange Server preventing connectivity.

Enable Remote Users

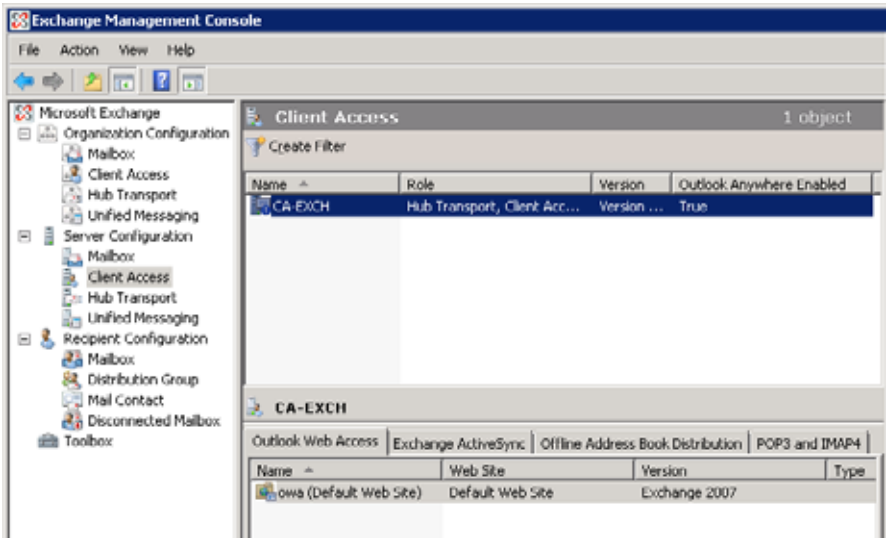
Polycom Conferencing for Outlook supports both H.323 clients (Polycom HDX systems) and Microsoft Office Communicator clients (see "Polycom-enabled Unified Communications" on page 19).

While the Polycom Conferencing for Outlook experience for H.323 and Office Communicator users inside the enterprise network is similar, the experience of remote users is slightly different depending on the deployment. Specifically:

- Polycom HDX system to Office Communications Server calls traversing an Edge Server are not supported. Thus, while it is possible to configure a SOHO Polycom HDX system so that it can view a particular calendar, the function to click a link to join a meeting will not work.
- Polycom HDX system H.323 calls are supported if the SOHO Polycom HDX system is registered to a Polycom VBP-S or VBP-S/T device which proxies the Polycom HDX system's registration to a Polycom CMA system gatekeeper inside the enterprise network.

To ensure that remote users can create and receive meeting invitations:

- Verify the Exchange Server servicing any external connections has Outlook Anywhere enabled:



Configure the Polycom the Infrastructure Mailbox and Devices

Polycom infrastructure devices (Polycom RMX, Polycom DMA, and Polycom RSS) monitor a single Exchange mailbox that is automatically scheduled into Polycom Conferencing for Outlook meetings.

Polycom infrastructure devices respond to meeting invitations sent to this address and provide accept / decline feedback to the meeting organizer.

The Polycom infrastructure account will always accept meeting invitations except when a conflict in Virtual Meeting Room numbers exists. These numbers are randomly generated by the Polycom Conferencing Add-in for Outlook and are unlikely to collide. If this occurs, the meeting organizer must cancel the meeting and send a new invitation. For details on other scenarios that may cause the Polycom DMA system or Polycom RMX system to reject meeting invitations, please see the Administrator Guides for those products.

Notes

- The Polycom infrastructure account's acceptance of a meeting is not capacity-aware. It is possible to schedule more participants into conferences than the infrastructure can support, so the administrator must carefully plan a deployment to ensure appropriate resources are in place.
- The Polycom Conferencing Add-in for Outlook generates random Virtual Meeting Room (VMR) identification numbers. It does not permit scheduling of static meeting rooms that use the same VMR numbers recurrently.

Complete the following tasks to set up your Polycom Infrastructure Integration

- "Create the Polycom Infrastructure Account and Mailbox" on page 55
- "Configure Microsoft Exchange Integration with Polycom RMX Systems" on page 56
- "Configure Calendaring Settings for Polycom DMA System" on page 58
- "Configure Calendaring Settings for Polycom RSS System" on page 59

Task 1: Create the Polycom Infrastructure Account and Mailbox

In Microsoft Exchange, create a standard user mailbox and account, using an email address such as **PolycomConferencing@companya.com**. Polycom infrastructure devices (Polycom RMX system, Polycom DMA system, and RSS) will monitor this account.

Polycom Infrastructure Mailbox Requirements:

- **A standard User Mailbox that is dedicated to Polycom use**.

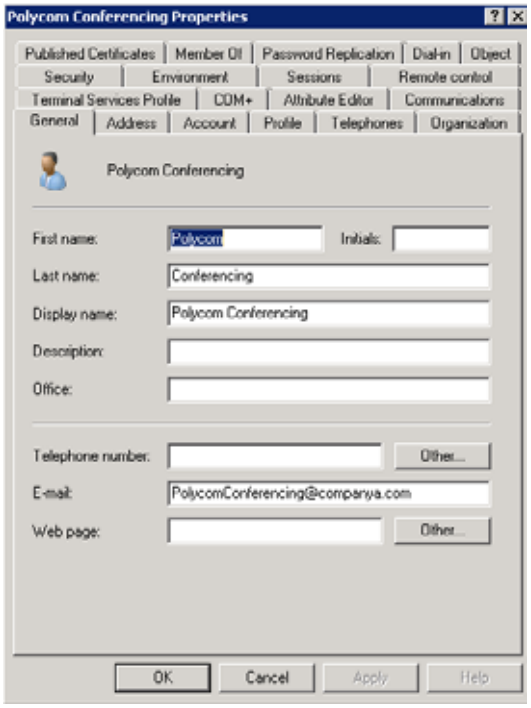
  You **cannot** use a room mailbox for the Polycom infrastructure mailbox. A dedicated mailbox is important because the Polycom DMA system deletes all messages from the Inbox when it checks this mailbox for meeting invitations.

- **A password that is set to never expire**.

  For organizations where a permanent password is not possible, the password for the account will need to be re-entered in each infrastructure device whenever it expires or is changed by the Active Directory administrator.

This e-mail account is automatically included in meetings created Polycom Conferencing for Outlook, see Figure 3-1 for an example of configuring a Polycom infrastructure mailbox.

Figure 3-1 *Example of a Polycom infrastructure account.*



Task 2: Configure Microsoft Exchange Integration with Polycom RMX Systems

The Polycom RMX system monitors the Exchange account you configured in "Configure the Polycom the Infrastructure Mailbox and Devices" on page 54.

The Polycom RMX system's Gathering Phase feature depends on the Polycom RMX system's ability to directly access the Exchange server mailbox to determine information such as the name of a given meeting, and what attendees are participating.

*Polycom RMX 2000/4000 Administrator's Guide.***To configure Exchange integration with a Polycom RMX system:**

1. Using a Web browser, connect to the RMX.
2. Select **Setup > Exchange Integration Configuration**.

   The **Exchange Integration Configuration** dialog displays.
3. Mark the **Enable Service** check box.
4. Complete the fields listed in Table 3-1.

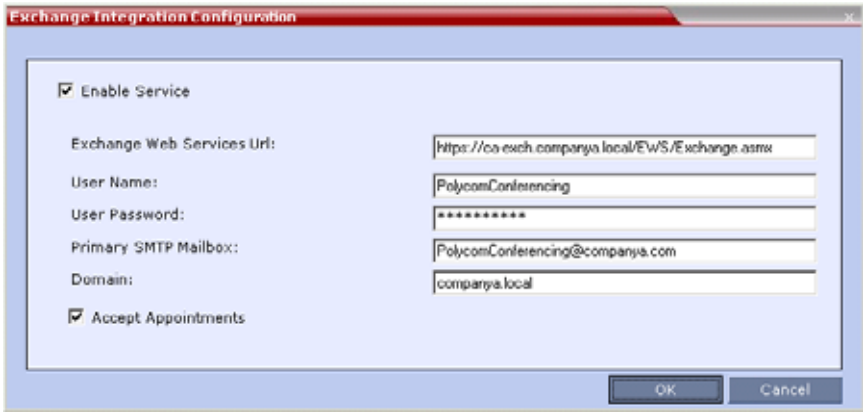
Table 3-1 *Configure Exchange integration in the RMX system.*

Exchange Web Services Url	Specify the full URL path to the Exchange Web Service, including the Exchange.asmx service on the Exchange server.
Domain	This is the logon domain of the user in either NETBIOS or DNS name notation. For example, in an Active Directory domain named companya.local with a NETBIOS name of COMPANYA you could enter either companya.local or COMPANYA.
User Name	This is the Active Directory account's user name only, with no domain information included
Password	The password for the user account.
Primary SMTP Mailbox	This must match the **Primary SMTP Address** for the account in Exchange (one account may have multiple associated SMTP addresses). This is displayed as the **Mail** field in Active Directory.

5. Mark the **Accept Appointments** check box, if your deployment does not include a DMA system, shown in Figure 3-2.

   If your deployment includes a DMA system, leave the **Accept Appointments** check box unchecked, shown in Figure 3-3. When a DMA system is present, it accepts appointments on behalf of the RMX.

Figure 3-2 *Example Polycom RMX system and Microsoft Exchange Integration without a DMA system.*



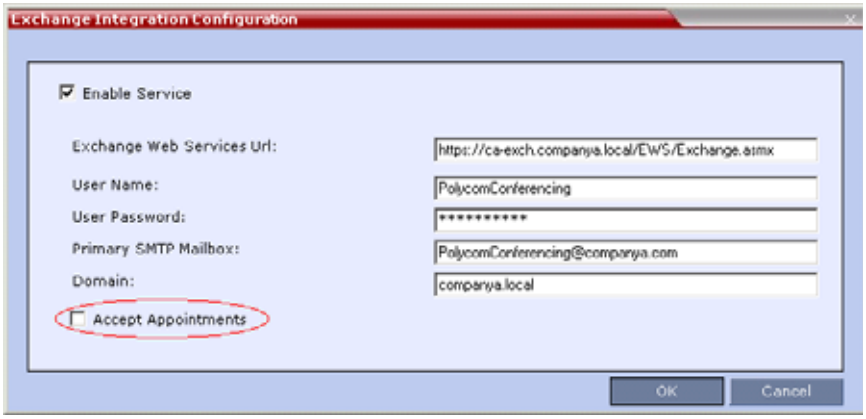
Tip

You can use the Microsoft Exchange Management shell to list the full Exchange Web Services URL.

Use a command prompt to navigate to the installation directory of the Microsoft Exchange Management shell, and type:
`get -WebServicesVirtualDirectory |fl`.

The Exchange Web Services URL is included in the returned list.

Figure 3-3 *RMX configuration with Exchange when using a DMA system.*



Task 3: Configure Calendaring Settings for Polycom DMA System

The DMA system needs to subscribe to the Exchange Server to receive notifications when meeting invitations are sent. It monitors the Polycom infrastructure account you created, see "Configure the Polycom the Infrastructure Mailbox and Devices" on page 54.

Be sure you have properly configured DNS before continuing, see "Configure DNS Entries Polycom Conferencing for Outlook" on page 51 for more information.

To configure calendar settings for the DMA system:

1. In a Web browser, connect to the DMA system.
2. Go to **Configuration > Conference Setup > Calendaring Service**.
3. Check the **Enable Calendaring Service** check box.
4. Specify the login credentials for the system on the Exchange server. Use the Polycom infrastructure account you configured, see "Configure the Polycom the Infrastructure Mailbox and Devices" on page 54.
5. If you have multiple Exchange servers behind a load balancer, under **Accept Exchange notifications from these additional IP addresses**, add the IP address of each individual Exchange server.
6. Click **Update**.

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

Figure 3-4 *Example Polycom DMA system and Microsoft Exchange integration.*

Task 4: Configure Calendaring Settings for Polycom RSS System

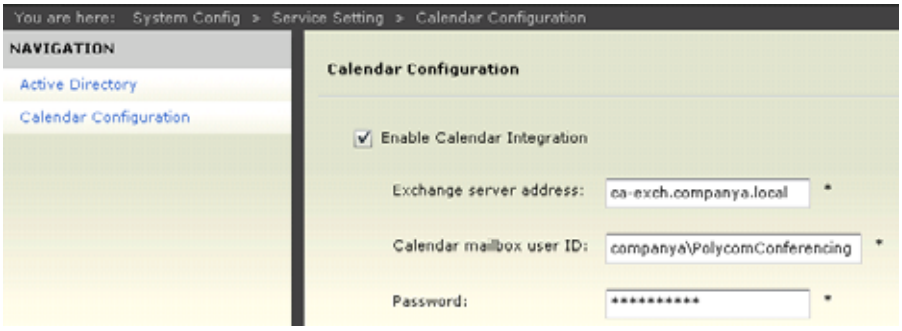
The Polycom RSS system needs to subscribe to the Exchange server to receive notifications of which meeting invitations have requested that the meeting be recorded.

It monitors the Polycom infrastructure account you created, see "Configure the Polycom the Infrastructure Mailbox and Devices" on page 54.

To configure calendar settings for a Polycom RSS system:

1. In a Web browser, connect to the RSS system.
2. Go to **System Config > Service Setting > Calendar Configuration**.
3. Check the **Enable Calendar Integration** check box.
4. Complete the provided fields, see the RSS documentation for more details.

Figure 3-5 *Example Polycom RSS system and Microsoft Exchange integration.*



Configure Mailboxes for Room-based HDX Systems

You need to configure an Exchange room mailbox and an Active Directory account (used to authenticate with Exchange) for each room-based HDX in your deployment.

Note In many environments, User and Room accounts are likely to already be configured. However, room mailboxes and accounts associated with a room-based HDX need additional configuration.

The Room Mailbox (sometimes referred to as the Resource Mailbox) is scheduled via the Outlook client when users wish to hold a meeting in the room. Scheduling a video-enabled Polycom Conferencing for Outlook conference uses the same workflows as reserving a conference room for a meeting without video. The Polycom HDX system located in the conference room monitors the Exchange calendar of this Room object to view the meetings scheduled for the conference room, both video-enabled and not.

You can configure mailboxes for HDX room systems in three ways, see Table 3-2.

1. Enable the user account associated with the room mailbox.

   The enabled Active Directory account can be used to authenticate with Polycom CMA system for automatic provisioning if the same credentials are used for both the Provisioning Service and Calendaring Service configurations in the Polycom HDX system.

2. Associate a service account to a single mailbox and grant that account full manage permissions.

3. Associate a service account to multiple mailboxes and grant that account full manage permissions.

By default, Room Mailboxes are linked to disabled Active Directory accounts. If your company's policy prohibits enabling the Active Directory accounts linked to Room Mailboxes, see "Option 2: Use a Service Account with a Single Room Mailbox" on page 64 or "Option 3: Use a Single Service Account for Multiple Room Mailboxes" on page 66.

Table 3-2 *Available features with different HDX room mailbox configurations.*

	An Exchange mailbox with enabled user account	**An Exchange mailbox with a disabled user account managed by a service account**	**Multiple Exchange mailboxes with disabled user accounts managed by a single service account**
Polycom Conferencing for Outlook	✓	✓	✓
Presence	✓ (either with CMA or Office Communications Server)	✓ (only with Office Communications Server)	✘
CMA Automatic Provisioning	✓	✘	✘
CMA Softupdate	✓	✘	✘

Note If your environment includes both a Polycom CMA system and Office Communications Server, presence and directory are provided by Office Communications Server.

Option 1: Enable the user account for the room mailbox

This section assumes you have already created the room mailbox.

Task 1: Enable the user account associated with the room mailbox

To enable the user account for a room mailbox:

1. In Active Directory, enable the account associated with the room mailbox.
2. Set the user account password to never expire.

   For organizations where a permanent password is not possible, the password for the account will need to be re-entered in each infrastructure device whenever it expires or is changed by the Active Directory administrator.

Task 2: Modify the room mailbox settings

The Subject and Description information needs to be included in the meeting invitation (some default Exchange configurations hide this information). The Polycom HDX system uses this data to display information and complete calls.

Optionally, you can also add the organizer's name to the meeting invitation.

You can modify these settings using Microsoft Exchange Powershell or Microsoft Office Web Outlook.

For details on using Microsoft Exchange Powershell, see http://technet.microsoft.com/en-us/library/bb123778(EXCHG.80).aspx

To use Microsoft Exchange Powershell to modify the mailbox settings:

1. View the settings for the Room Mailbox.

   `Get-MailboxCalendarSettings <ExchangeMailbox> | fl`

   For example: `Get-MailboxCalendarSettings zeusroom | fl`

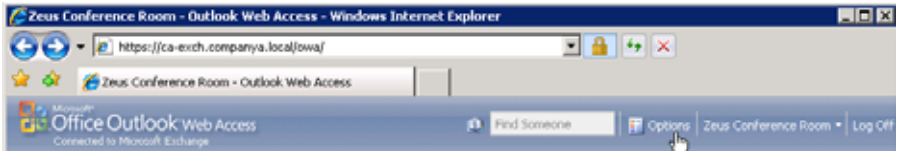
   - By default, the `DeleteSubject` value is set to `True`. This setting must be set to **`False`**.
   - By default, the `DeleteComments` value is set to `True`. This setting must be set to **`False`**.
   - By default, the `AddOrganizerToSubject` value is set to `True` and will add the organizer's name to the subject line. Changing this setting is optional.

2. Set the Room Mailbox properties (0 configuration equates to False):

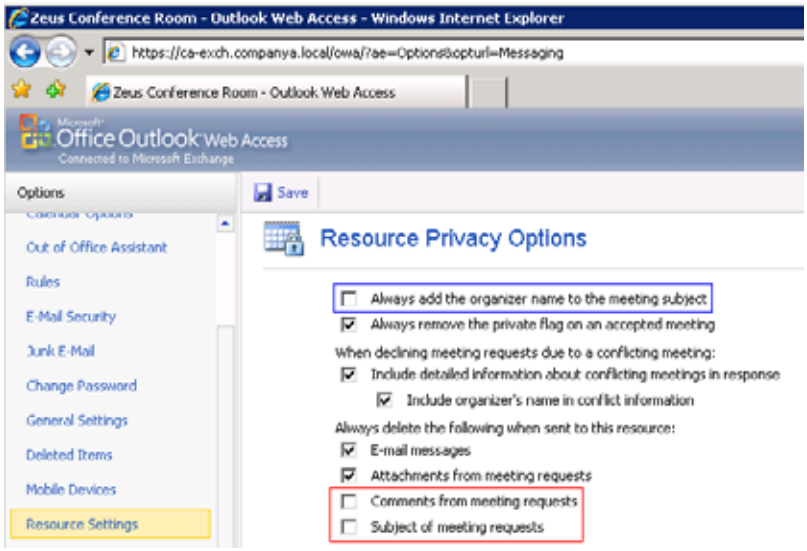
```
Set-MailboxCalendarSettings -id <ExchangeMailbox> -DeleteComments:0 -DeleteSubject:0
-AddOrganizerToSubject:0
```

To use Office Outlook Web Access to Configure the Mailbox Settings:

1. Log in to Outlook Web Access using the Room's credentials.
2. Click **Options**.



3. Select **Resource Settings** from the Options bar and scroll down to Resource Privacy Options.



The two settings highlighted in red correspond to the required Exchange Powershell commands above - the blue setting corresponds to the optional setting.

Option 2: Use a Service Account with a Single Room Mailbox

This section assumes you have already created the room mailbox.

If your organization has a requirement to keep room accounts disabled, you can set up an Active Directory user account with rights to manage the Room Mailbox in Exchange.

This configuration results in two accounts in the Microsoft deployment:

- One Primary account that is *disabled* in Active Directory *with* an associated Exchange Mailbox.
- One Service account that is *enabled* in Active Directory *without* a directly assigned Exchange Mailbox.

Task 1: Create the service account

This Active Directory account may be named starting with SRV-, or another naming scheme fitting with your organization's deployment. The configuration is similar to any standard user account, and no Exchange mailbox is directly associated.

To create the service account for your room mailbox:

1. Use Active Directory to create the service account you will use to manage the room mailbox.

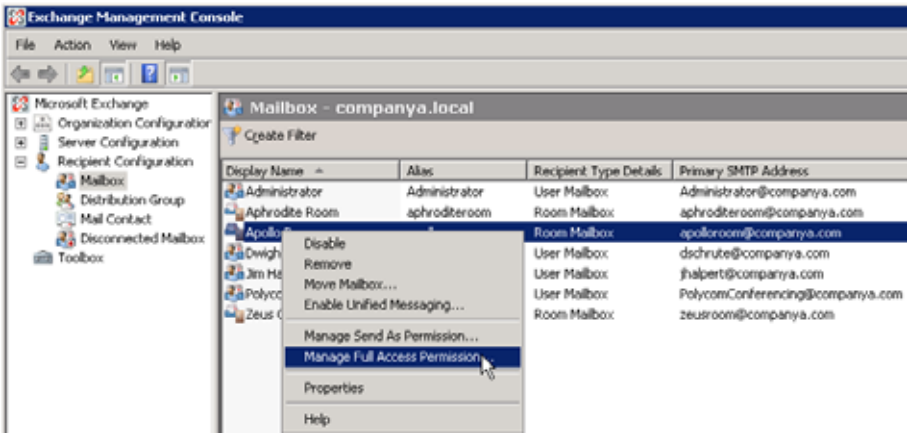
Task 2: Grant the service account the permission to manage the Room Mailbox

You can do this either with the Exchange Management Console of the Exchange Management Shell.

To Use the Exchange Management Console to grant permission:

1. Navigate to the resource mailbox to which you want to grant permissions.
2. Right-click the mailbox and select **Manage Full Access Permission**.

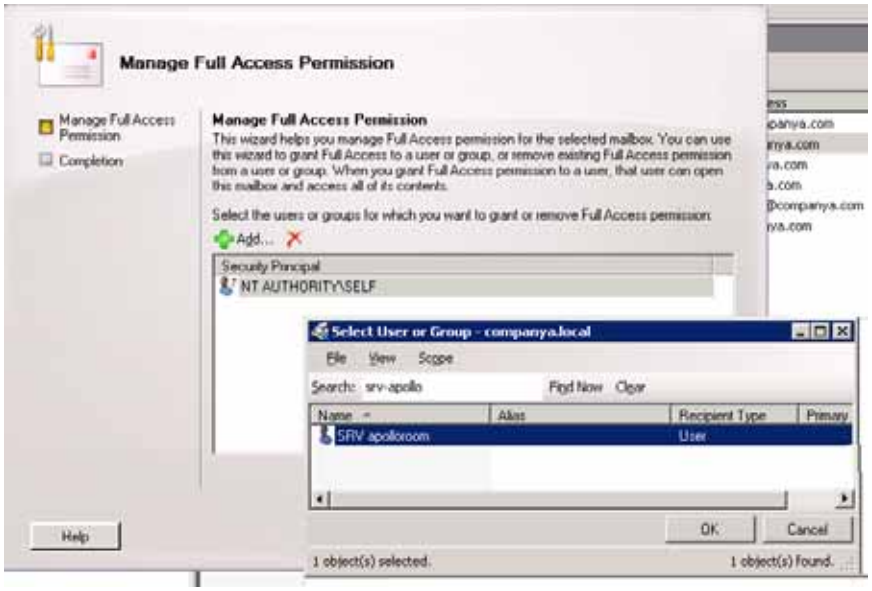
Figure 3-6 *Select Manage Full Access Permission of the Room Mailbox.*



3 In the **Manage Full Access Permission** dialog box, click **Add** and add the Active Directory service account to the list.

In Figure 3-7, the `SRV-apolloroom` is a service account that has no directly assigned Exchange Mailbox, but it is given permission to manage the Room Mailbox assigned to the `apolloroom` user.

Figure 3-7 *Select the service account you created.*



To Use the Exchange Management Shell to Grant Permissions:

- Run the following Exchange Management Shell command to grant the service account full access permissions for the Room Mailbox:

```
Add-MailboxPermission -Identity '<conference room primary
SMTP address>' -User
'<domain>\<hdxActiveDirectoryAccountUserName>' -AccessRights
'FullAccess' –InheritanceType ‘All’
```

Option 3: Use a Single Service Account for Multiple Room Mailboxes

You can use one service account for all Polycom HDX systems in the Polycom Conferencing for Outlook deployment.

Note If you create one service account for multiple room mailboxes, you will not be able to take advantage of presence information, see “Available features with different HDX room mailbox configurations.” on page 61.

The steps for this approach are the same as mentioned in “Option 2: Use a Service Account with a Single Room Mailbox” on page 64, with the exception that you can grant the same service account permission to manage multiple mailboxes.

In Figure 3-8, the SRV-AllHDX-CompanyA service account is being used to manage multiple conference rooms. Only the association between Aphrodite and SRV-AllHDX-CompanyA is shown, but this same association could be duplicated for other rooms. For example, SRV-AllHDX-CompanyA could manage dozens of conference rooms within Company A, such as the Poseidon Room, the Hestia Room, and more.

Figure 3-8 *Using a service account for all HDX conference rooms.*

Configure Mailboxes for Polycom HDX Desktop Systems

Each HDX desktop system in your deployment needs to be configured to use an individual user's Active Directory account and Exchange Mailbox for authentication with Exchange.

Optionally, the Active Directory account can be used to authenticate with Polycom CMA system for automatic provisioning.

There is no additional Exchange configuration necessary to for user accounts to be integrated with an HDX system.

Configure Polycom HDX System Calendaring Settings

You must configure calendar settings for each HDX system in your deployment.

When configuring calendar settings for a Polycom HDX, you need to specify the Room Mailbox and the Active Directory user name for the service account that manages the mailbox.

If you are using a Polycom CMA system, these settings can be dynamically managed, see "(Optional) Configure Polycom CMA System Automatic Provisioning of Calendaring Service Settings on Polycom HDX systems" on page 72 instead.

To configure the calendar service on an HDX system:

1. In a Web browser, connect to the HDX system.
2. Go to **Admin Settings > Global Services > Calendaring Service**.
3. Check the **Enable Calendaring Service** check box.
4. Complete the fields listed in Table 3-3.

   For complete documentation on configuring calendaring settings for an HDX system, see the *Administrator's Guide for Polycom HDX Systems*.

Table 3-3 *Calendar Settings in the Polycom HDX system.*

Server Address	This is the fully qualified domain name (FQDN) of the Microsoft Exchange Client Access Server. If your organization has multiple Client Access Servers behind a network load balancer, then the Exchange Server Address would be the FQDN of the Client Access Servers' Virtual IP Address. If required, an IP address can be used in place of an FQDN but Polycom recommends using the same FQDN that is used for Outlook clients.
Domain	This is the logon domain of the user in either NETBIOS or DNS name notation. For example, in an Active Directory domain named companya.local with a NETBIOS name of COMPANYA you could enter either companya.local or COMPANYA.
User Name	This is the Active Directory account's user name only, with no domain information included
Password	The password for the user account.
Mailbox (Primary SMTP)	This must match the **Primary SMTP Address** for the account in Exchange (one account may have multiple associated SMTP addresses). This is displayed as the **Mail** field in Active Directory.

5 Click Update.

Example Calendar Settings

Figure 3-9 shows the configuration using the method described in "Option 1: Enable the user account for the room mailbox" on page 62. The zeusroom Active Directory account is enabled and no service accounts are required. As a User, Dwight's Active Directory account is enabled as well.

Figure 3-9 *Using an enabled user account assigned to a room mailbox.*

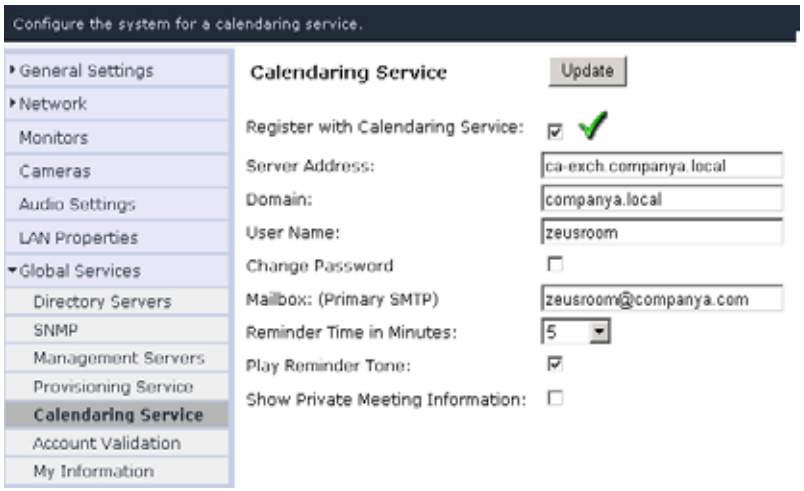


Figure 3-10 shows the ‘individual service accounts’ strategy discussed in “Option 2: Use a Service Account with a Single Room Mailbox” on page 64. The integration between the apolloroom Mailbox and the SRV-apolloroom service account is reflected in the HDX as below.

Figure 3-10 *Using a service account to manage a single mailbox.*

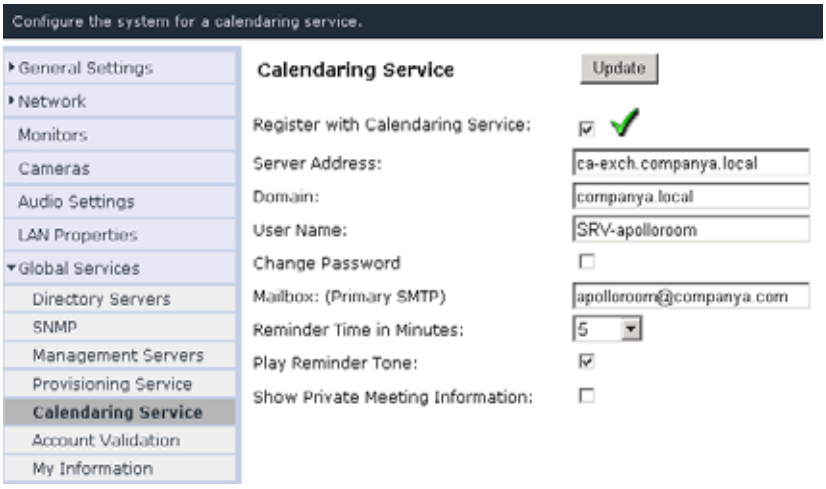


Figure 3-11 shows, the ‘shared service account for all HDXs’ strategy discussed in “Option 3: Use a Single Service Account for Multiple Room Mailboxes” on page 66. The integration between the Aphrodite Room and the SRV-AllHDX-Company A service account is shown. Remember that this service account may also be managing other Room Mailboxes simultaneously.

Figure 3-11

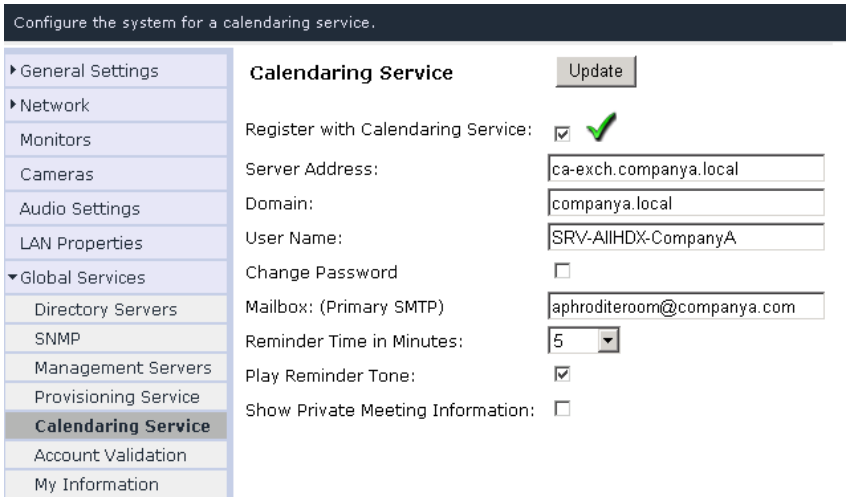


Figure 3-12 shows the calendar settings of the Polycom HDX system assigned to user Dwight Schrute, which reside on the LAN inside Company A's corporate network.

Figure 3-12 *User-based Calendar Settings in the Polycom HDX System*

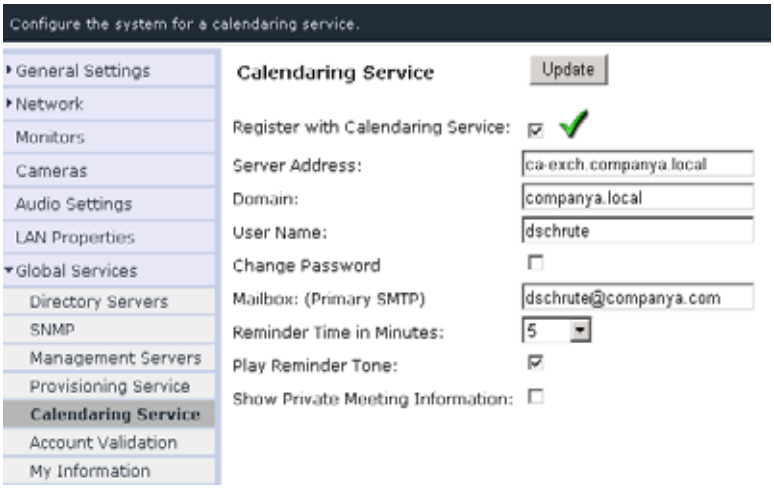
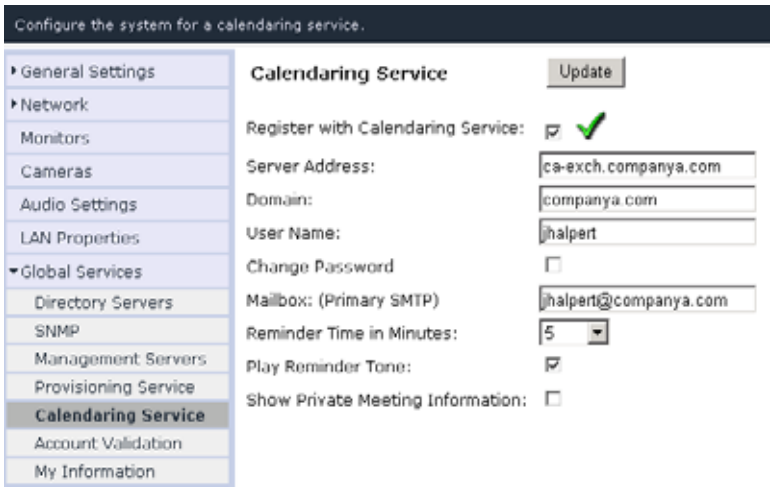


Figure 3-13 shows the configuration for a SOHO user. When configuring a remote HDX user, be sure to use a publicly-routable Exchange server address, see Figure 3-13. Microsoft Outlook Anywhere must be enabled, see "Enable Remote Users" on page 53.

Figure 3-13 *Calendar configuration for a SOHO User.*



(Optional) Configure Polycom CMA System Automatic Provisioning of Calendaring Service Settings on Polycom HDX systems

You can use the Polycom CMA system to automatically provision a Polycom HDX system when using dynamic management mode, see "Deploying Dynamic Device Management" on page 4.

To use the Polycom CMA system to automatically provision a Polycom endpoint system, the endpoint system must use the same credentials (username and password) to access both the Exchange server and the Polycom CMA system. Only then can the Polycom CMA system automatically provision a calendaring service-enabled endpoint system.

See the *Polycom CMA System Operations Guide* for more information.

Note You must use an enabled resource account (Room Mailbox) in order to take advantage of CMA Automatic Provisioning, see "Configure Mailboxes for Room-based HDX Systems" on page 60

Configure and Install the Polycom Conferencing Add-In

The Polycom Conferencing Add-In software and its templates must be installed on each Microsoft Outlook client.

For complete documentation, see the *System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook*.

Complete the following tasks:

- "Configure Polycom Conferencing Add-in Preferences For Installation to Client PCs" on page 72
- "Install Polycom Conferencing Add-in for Outlook to Client PCs" on page 73
- "Deploy Customization Files" on page 73
- "Test Polycom Conferencing for Outlook Deployment" on page 73

Task 1: Configure Polycom Conferencing Add-in Preferences For Installation to Client PCs

Administrators can configure the client experience of the Polycom Conferencing Add-in before deploying the client to users. For details on how to configure preferences as an administrator, refer to the *System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook*.

Task 2: Install Polycom Conferencing Add-in for Outlook to Client PCs

The Conferencing Add-in can be installed in a number of ways, depending on the administrator's preference. After customizing preferences as described in Task 1:, the administrator can provide the file to users via existing software deployment processes, using a link to a network location where the file resides, by using a software installation program like Microsoft SMS, or by using a Group Policy Object. For specifics regarding your environment's preferred software delivery method, consult the documentation for your software delivery product.

For an example deployment method using Microsoft Active Directory and Global Policy, refer to the *System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook.*

Task 3: Deploy Customization Files

After the installation described in Task 2:, the customization files created in Task 1: can be deployed to the appropriate folder locations on client PCs. The Add-in must already be installed on the client PC, to ensure these file paths have been created. For an example of one possible deployment method using Microsoft Active Directory and Global Policy, refer to the *System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook.*

Task 4: Test Polycom Conferencing for Outlook Deployment

- Walk through scheduling and joining a meeting.
- For more details on the on-screen experience with an Polycom HDX system, please see the Polycom HDX system documentation.

A

Polycom HDX System Configuration Files

The following table lists all of the **.dat** files that the Polycom HDX system can read from the USB boot device.

You can either put these files in a `/usb_oob/general` directory or in a `/usb_oob/<serial_number>` directory on a USB storage device.

- Provisionable configuration files in the `/usb_oob/general` directory are copied to the Polycom HDX system unconditionally.
- Provisionable configuration files in the `/usb_oob/<serial_number>` directory are copied to Polycom HDX system only when the `<serial_number>` matches the serial number of the endpoint.
- If the same file exists in both the `/usb_oob/general` and `/usb_oob/<serial_number>` directories, the copy in the `/usb_oob/<serial_number>` directory takes priority.

`.dat` File Name	Description	Value Range	Content Example
langwithcntry	Language and country	Text string	English/en
connecttomylan	Enable or disable LAN interface	False, True	
lanportspeed	LAN speed	Auto, 10_Mbps, 100_Mbps, 1000_Mbps	
landuplexmode	LAN duplex	Auto, Full, Half	
dot1xenabled	Enable or disable 802.1X authentication	False, True	
dot1xid	802.1X authentication user id	Text string	johnsmith
dot1xpwd	802.1X authentication password	Text string	johnsmithpassword
vlanmode	Enable or disable VLAN	False, True	
vlanid	VLAN ID	Integer in [2,4094]	100

.dat File Name	Description	Value Range	Content Example
dhcp_flg	Enable or disable DHCP client	Client, Off	
hostname	Host name of the Polycom HDX system	Text string	hdx334
userdomain	Domain of the user account used to log into the provisioning server	Text string	polycom.com
domainname	Domain of the Polycom HDX system, which will be set by the network itself if DCHP is provisioned	Text string	
ipaddress	IP address of the Polycom HDX system	IP address	172.18.1.222
subnetmask	Subnet mask of the Polycom HDX system		255.255.255.192
defaultgateway	IP address of the default router	IP address	172.18.1.65
dnsserver	DNS server	IP address	172.18.1.15
dnsserver1	Alternate DNS server	IP address	
dnsserver2	Alternate DNS server	IP address	
dnsserver3	Alternate DNS server	IP address	
provisionserveraddress	IP address of the Polycom CMA server	IP address or host name	polycomCMA.polycom.com
ldapuserid	LDAP user id	Text string	johnsmith
ldappassword	LDAP password	Text string	johnsmithpassword

B

Exchange Calendar Polling Information

Polycom HDX System

When actively viewing the endpoint's calendar onscreen, the Polycom HDX system polls the Exchange server for updates every 20 seconds. When viewing any other screen, or when the Polycom HDX system is in standby, polling occurs every five minutes.

Polycom DMA System

Polycom DMA system uses the Push Notification feature of Exchange Web Services to receive notifications of new or updated calendar events in the Polycom Conferencing Mailbox as they are created. Upon receiving a push notification, Polycom DMA system connects to Exchange to download the meeting details. When doing this, Polycom DMA system processes the new event and also requests a refreshed view of all calendar events occurring in the next 24 hours.

In the absence of these notifications, Polycom DMA system connects to the Exchange server every five minutes to retrieve the number of events scheduled to occur on the current calendar day, which it reports on the Dashboard under **Calendaring Servic**e as **Meetings scheduled today**.

Polycom RMX System

The Polycom RMX system polls the Exchange server for updates every 15 seconds. When polling, the RMX considers events two hours in the past and 24 hours into the future.

Polycom RSS System

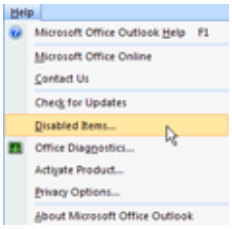
The Polycom RSS system polls the Exchange server every 30 seconds.

C

Troubleshooting

No longer able to access the Polycom Conferencing Add-In

It is possible for the Polycom Conferencing Add-In to become disabled. If this occurs, navigate to **Help > Disabled Items** in Microsoft Outlook and enable the Polycom Conferencing Add-In again.



Polycom HDX systems display conference times but no details

Most likely, the Exchange Powershell commands to change the default Exchange behavior of deleting meeting information after acceptance have not been completed. Review the Exchange Powershell commands in "Modify the room mailbox settings" on page 62 and verify that they have been performed correctly.

Index