Microsoft Outlook Calendar Integration for the IM and Presence Service, Release 12.5(1)SU2 to 12.5(1)SU8

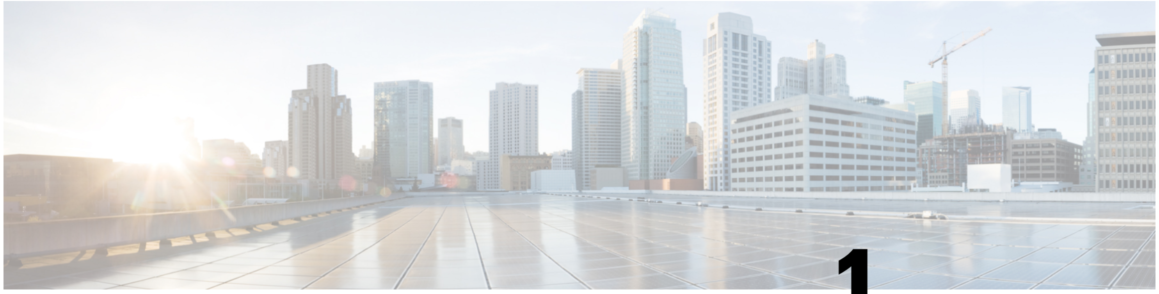
First Published: 2020-02-03

Last Modified: 2023-07-20

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Preface

Introduction

Calendar integration with the IM and Presence Service allows users to incorporate their calendar and meeting status from Microsoft Outlook into their availability status on IM and Presence Service.

New and Changed Information

The following table provides an overview of the significant changes to the features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior in Unified Communications Manager and IM and Presence Service

Feature or Change	Description	See	Date
Initial Release of Document for Release 14	—	—	March 31, 2021
Initial Release of Document for Release 14SU1	—	—	October 27, 2021
Initial Release of Document for Release 14SU2	—	—	June 16, 2022

Audience

This publication is for experienced users who configure and maintain Microsoft Exchange integration with the IM and Presence Service.

Book Structure

This guide contains the following chapters:

Chapter	Title	Description
1	Preface, on page 1	This chapter contains information on the book structure, audience, and purpose of this guide.
2	Introduction, on page 7	This chapter introduces the Microsoft Outlook calendar integration feature for the IM and Presence Service.
3	New and Changed Information, on page 1	This chapter is about new and changed information.
4	Planning for Calendar Integration, on page 11	This chapter contains information on the prerequisites so that you can plan your calendar integration.
5	Configure Microsoft Exchange, on page 35	Refer to this chapter only if you are connecting to an on-premise Microsoft Exchange server for Outlook calendar integration. This chapter describes how to configure your Exchange server for the integration.
6	Configure Microsoft Office 365, on page 63	Refer to this chapter only if you are connecting to a cloud-hosted Office 365 server for Outlook calendar integration. This chapter describes how to configure your Office 365 server for the integration.
7	Configure the IM and Presence Service, on page 67	Refer to this chapter to configure the IM and Presence Service for Outlook calendar integration. Use this chapter regardless of whether you are connecting to an on-premise Exchange server or a cloud-hosted Office 365 server.
8	Troubleshooting Exchange Calendaring Integrations, on page 93	This chapter describes troubleshooting tasks and fixes for common problems.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information helps you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 2

New and Changed Information

New and Changed Information

The following table provides an overview of the significant changes to the features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 2: New Features and Changed Behavior in Unified Communications Manager and IM and Presence Service

Feature or Change	Description	See	Date
Initial Release of Document for Release 12.5(1)SU8	—	—	July 20, 2023
CSCwd62307	Basic Authentication Type for Office 365 server is deprecated.	Configure a Presence Gateway, on page 68	July 20, 2023
Initial Release of Document for Release 12.5(1)SU2	—	—	February 3, 2020
Calendar Integration with Office 365 Support for OAuth 2.0 authentication	The IM and Presence Service's Calendar Integration with Office 365 feature is enhanced to support the usage of OAuth tokens for authenticating to the Office 365 server.	Configure a Presence Gateway, on page 68	February 3, 2020

CHAPTER 3

Introduction

Overview

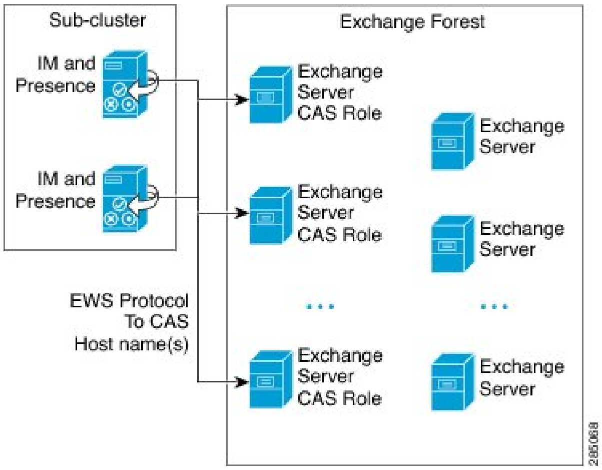
Microsoft Outlook calendar integration with the IM and Presence Service allows users to incorporate their calendar/meeting status in Microsoft Outlook into their availability status on the IM and Presence Service server. This integration can be accomplished by connecting the IM and Presence Service to an on-premises Microsoft Exchange server or a hosted Office 365 server.

Deployment

Exchange Web Services

Exchange Web Services (EWS) allows interaction with Microsoft Exchange mailboxes and contents over HTTP. EWS provides access to much of the same data that is made available through Microsoft Outlook. EWS moves several responsibilities from the client computer to the server.

Figure 1: Microsoft Exchange Integration with the IM and Presence Service over EWS



Microsoft Outlook Calendaring States on the IM and Presence Service

Microsoft Outlook integration with the IM and Presence Service via Microsoft Exchange or Office 365allows users to incorporate their calendar/meeting status in Microsoft Outlook into their availability status on the IM and Presence Service. The table below shows the reachability mappings, and how the IM and Presence Service correlates the status of meetings (as shown in Microsoft Outlook calendar) in the availability status of users on the IM and Presence Service.

Table 3: Aggregated Availability State Based on Calendar State

Microsoft Outlook State	IM and Presence Service State
Free/Tentative	Available
Busy	In a meeting
Out-of-Office[1]	Away
Away[2]	Away

[1] Microsoft Outlook 2007 and Microsoft Outlook 2010 desktop client.

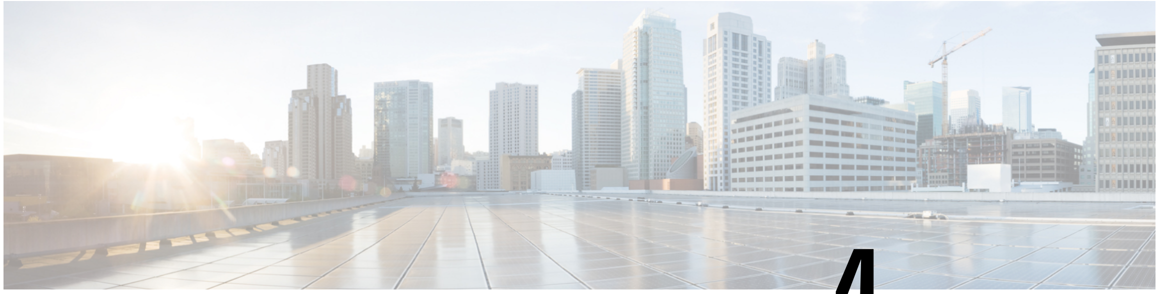
[2] Microsoft Outlook Web Access (OWA) 2010.

Restrictions and Limitations

The following are restrictions and limitations for integrating the IM and Presence Service with Microsoft Exchange:

- You can add, update, or delete one or more EWS servers with no maximum limit. However, the **Troubleshooter** on the **Presence Gateway Configuration** window is designed to only verify and report status of the first 10 EWS servers that you configure.
- This release of the IM and Presence Service does not support the Exchange autodiscover service. The autodiscover service assumes that a load-balancing mechanism is already in place across the Client Access Server (CAS) or servers.
- Upon configuring Exchange server or an Office 365 server as Presence Gateway the Jabber Clients will not be able to set **'In a meeting’** status when they have a meeting received from their local Outlook. The **'In a meeting'** status can only come via the Presence Gateway. If the Presence Gateway goes down for any reason the clients will not be able to set **'In a meeting'** status .

Note In order to have a **‘In a meeting'** status set you must restore service for the Presence Gateway.



CHAPTER 4

Planning for Calendar Integration

Prerequisites

Before you configure Microsoft Outlook calendar integration with the IM and Presence Service, consult the compatibility matrix below and make sure that you have installed and configured the required components for this integration:

Table 4: Compatibility Matrix

Component	Install Compatible Version
Windows Server	
CiscoUnified Communications Manager	For Standard Deployments, the Cisco Unified Communicati release versions must match. As of Release 11.5(1)SU4, the IM and Presence Centralized your IM and Presence cluster using a different version than
IM and Presence Service	For Standard Deployments, the Cisco Unified Communicati release versions must match. As of Release 11.5(1)SU4, the IM and Presence Centralized your IM and Presence cluster using a different version than
Microsoft Exchange Server 2007	Service Packs for Microsoft Exchange 2007 (SP1).
Microsoft Exchange Server 2010	Service Packs for Microsoft Exchange 2010 (SP1).
Microsoft Exchange Server 2013	Service Packs for Microsoft Exchange 2013 (SP1).
Microsoft Exchange Server 2016	Microsoft Exchange 2016
Microsoft Office 365	Refer to your Microsoft documentation for details on deplo

Component	Install Compatible Version
Active Directory	**Note** User names configured in Active Directory must b Cisco Unified Communications Manager.
A Third-Party Certificate OR Certificate Server	One or the other of these is required to generate the certificates **Note** Microsoft Exchange integration with IM and Preser RSA 1024 or 2048 bit keys and SHA1 and SHA25

Exchange Server 2007, 2010, 2013 and 2016 support Exchange Web Services (EWS).

Configuration Considerations

This book contains configuration tasks that describe how to configure calendar integration between the IM and Presence Service and Microsoft Outlook for an on-premise Microsoft Exchange deployment or a hosted Office 365 deployment. Use the table below to determine which chapters to use for your deployment.

Table 5: Configuration Tasks for Microsoft Deployments

Microsoft Deployment	Complete these configuration chapters...
Microsoft Exchange (2007, 2010, 2013, 2016)	• Configure Microsoft Exchange, on page 35 • Configure the IM and Presence Service, on page 67
Microsoft Office 365	• Configure Microsoft Office 365, on page 63 • Configure the IM and Presence Service, on page 67

Integration with Microsoft Exchange Server over Exchange Web Services

Microsoft Exchange Server 2007 introduced Exchange Web Services (EWS) for calendaring integration using a Simple Object Access Protocol-like (SOAP) interface to the Exchange Server.

When configuring your EWS Presence Gateway for Exchange integrations in the **Cisco Unified CM IM and Presence Service Administration** user interface, note the following:

- You can add, update or delete one or more EWS servers with no maximum limit. However, the Troubleshooter on the **Presence Gateway Configuration** window is designed to only verify and report status of the first 10 EWS servers that you configure.
- EWS Server gateways share the credentials (Account Name and Password) that you configure for the first EWS Server Gateway. If you change the credentials for one EWS Server Gateway, the credentials change accordingly on all of the configured EWS gateways.
- You must restart the Cisco Presence Engine after you add, update or delete one or more EWS servers for your configuration changes to take effect. If you add multiple EWS servers one after another, you can restart the Cisco Presence Engine once to effect all of your changes simultaneously.

Administrative Roles and Permissions in Exchange Server

Exchange Web Services (EWS) requires a special account to enable access to all user calendaring information. This account is referred to as the impersonation account.

Microsoft Exchange Server 2007

For a caller to access the email account of another user with Exchange Server 2007, the EWS integration requires an account with Impersonation permissions. The caller impersonates a given user account using the permissions that are associated with the impersonated account instead of the permissions that are associated with the account of the caller.

The impersonated account must be granted the **ms-Exch-EPI-Impersonation** permission on the Client Access Server (CAS) running Exchange 2007. This gives the caller the permission to impersonate a user email account using the CAS. In addition, the caller must be granted the **ms-Exch-EPI-MayImpersonate** permission on either the mailbox database or on the individual user objects in the directory.

Note that the Access Control List (ACL) for an individual user takes precedence over the mailbox database setting so that you can allow a caller access to all mailboxes in the database but if required, deny access on certain mailboxes in that database.

Microsoft Exchange Server 2010 and 2013

Microsoft Exchange Server 2010 and 2013 use Role-Based Access Control (RBAC) to assign permissions to impersonation accounts and allow users to perform tasks specific to their function in the organization. Depending on whether the user is an administrator, super user, or an end-user, there are two primary methods to apply RBAC permissions:

- Management role groups—Microsoft provides 11 default management role groups during the Exchange setup process with associated permissions specific to the role of the group. The Recipient Management and Help Desk, for example, are built-in role groups. Typically, super users who need to perform specific tasks are assigned to the relevant management role group and inherit the associated permissions. For example, a Product Support representative who needs to be able to modify the contact details of any user across the entire Exchange organization may be assigned as a member of the Help Desk management role group.

- Management role assignment policies—For normal users who are not administrators or super users, management role assignment policies control the specific mailboxes such users can modify. The **ApplicationImpersonation** role, when assigned to the user using the **New-ManagementRoleAssignment** cmdlet, enables an account to impersonate users in an organization to perform tasks on behalf of the user. The scope of the role assignments are managed individually using the **New-ManagementScope** cmdlet, and can be filtered to target specific recipients or specific servers.

Note With RBAC, you do not need to modify and manage the ACL as required for Exchange Server 2007.

Presence Gateway Configuration for Exchange Server Integrations

To support a large number of users (with EWS calendar integration enabled), the IM and Presence Service must distribute the load of EWS traffic among multiple Client Access Servers (CAS). The IM and Presence Service can connect to a number of CAS by way of EWS, and it uses the following round robin strategy to support the traffic load that it encounters:

- The first time that a user's calendar subscription is enabled, the user is assigned a CAS from a pool of eligible CAS hosts configured by the administrator.
- The user retains the assignment until their calendar subscription fails.
- If the user’s calendar subscription fails, the user is again assigned a CAS from the pool of eligible CAS hosts.

Known Issues with Exchange Web Services Integration

- See the Troubleshooting Exchange Calendaring Integrations, on page 93 chapter of this guide to learn about issues that are known to impact Exchange Web Services (EWS) integrations.
- See Issues Known to Impact Microsoft Exchange Integrations , on page 97.

Security Considerations

Windows Security Policy Settings

IM and Presence Service integration with Microsoft Exchange supports various authentication methods including Windows Integrated authentication (NTLM).

IM and Presence Service supports both NTLMv1 and NTLMv2 Windows Integrated authentication, with NTLMv2 used as the default.

Configuring the **Lan Manager authentication level** to **Send NTLMv2 response only. Refuse LM & NTLM** on the Windows domain controller enforces NTLMv2 authentication on the domain.

Note IM and Presence Service does not support NTLMv2 session security. Message confidentiality and integrity are provided by secure http (https).

Getting More Information

Cisco Unified Communications Manager and IM and Presence Service Documentation

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Microsoft Exchange 2007 Documentation

http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx

Microsoft Exchange 2010 Documentation

http://technet.microsoft.com/en-us/library/bb124558.aspx

Microsoft Exchange 2013 Documentation

http://technet.microsoft.com/en-us/library/bb124558%28exchg.150%29.aspx

Microsoft Active Directory 2008 Documentation

http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx

CHAPTER 5

Configure Microsoft Exchange for Calendaring Integration

Microsoft Exchange 2007 Configuration over Exchange Web Services

Before You Begin

Note that the steps required to configure Exchange Server 2007 differ depending on whether you use Windows Server 2003 or Windows Server 2008.

You must complete the following tasks when configuring access to mailboxes on the Exchange Server 2007. For detailed instructions, see the Exchange Server 2007 documentation at the following URL:http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx.

- Verifying Windows Security Settings, on page 18
- Grant Users Permission to Sign in to the Service Account Locally, on page 18
- Setting Impersonation Permissions at the Server Level , on page 20
- Granting Send As Permissions to the Service Account and User Mailboxes, on page 21
- Granting Impersonation Permissions to the Service Account and User Mailboxes, on page 22
- Verifying Permissions on the Microsoft Exchange 2007 Account, on page 23

Tip The IM and Presence Service only requires impersonation permissions on the account to enable it to log in to that account when it connects to the Exchange Server. Note that this account does not typically receive mail so you do not need to be concerned about allocating space for it.

Windows Security Policy Settings

IM and Presence Service integration with Microsoft Exchange supports various authentication methods including Windows Integrated authentication (NTLM).

IM and Presence Service supports both NTLMv1 and NTLMv2 Windows Integrated authentication, with NTLMv2 used as the default.

Configuring the **Lan Manager authentication level** to **Send NTLMv2 response only. Refuse LM & NTLM** on the Windows domain controller enforces NTLMv2 authentication on the domain.

Note IM and Presence Service does not support NTLMv2 session security. Message confidentiality and integrity are provided by secure http (https).

Verifying Windows Security Settings

Procedure

Step 1 On the Windows domain controller and server(s) running Exchange, choose **Start** > **Administrative Tools** > **Local Security Policy**.

Step 2 Navigate to **Security Settings** > **Local Policies** > **Security Options**.

Step 3 Choose **Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers**.

Step 4 Verify that the **Require NTLMv2 session security** check box is unchecked.

Step 5 If the **Require NTLMv2 session security** check box is checked, complete the following steps:

a) Uncheck the check box **Require NTLMv2 session security**.

b) Click **OK**.

Step 6 To apply the new security settings reboot the Windows domain controller and server(s) running Exchange.

Note The reboot is only required for servers on which a security policy configuration change was performed.

Grant Users Permission to Sign in to the Service Account Locally

Complete one of the following procedures to configure users to log in to the service account locally.

Before you begin

- For Exchange impersonation to work, all Microsoft Exchange servers must be members of the Windows Authorization Access Group.
- The service account should not be a member of any of the Exchange Administrative Groups. Exchange explicitly denies Impersonation for all accounts in those groups.

Configuring Microsoft Exchange 2007 on Windows Server 2003

Procedure

Step 1 Log in to the Exchange Server 2007 user interface using a service account that has been delegated the Exchange View Only Administrator role.

Step 2 In the left pane, under Security Settings, navigate to **Local Policies** > **User Rights Assignments**.

Step 3 In the right pane of the console, double-click **Allow Log On Locally**.

Step 4 Choose **Add User or Group** then navigate to the service account that you created and choose it.

Step 5 Choose **Check Names**, and verify that the specified user is correct.

Step 6 Click **OK**.

What to do next

Setting Impersonation Permissions at the Server Level , on page 20

Configuring Microsoft Exchange 2007 on Windows Server 2008

Procedure

Step 1 Log in to Exchange Server 2007 using a service account that has been delegated the Exchange View Only Administrator role.

Step 2 Choose Start.

Step 3 Type gpmc.msc.

Step 4 Choose Enter.

Step 5 Open the **Domain Controller Security Settings** window on the Exchange Server.

Step 6 In the left pane, under **Security Settings**, navigate to **Local Policies** > **User Rights Assignments**.

Step 7 In the right pane of the console, double-click **Allow Log On Locally**.

Step 8 Ensure that the **Define these policy settings** check box is checked.

Step 9 Choose **Add User or Group** and navigate to the service account that you previously created and choose it. Then click **OK**.

Step 10 Choose **Check Names**, and verify that the specified user is correct. Then click **OK**.

Step 11 Click **Apply** then click **OK** in the **Allow Log On Locally Properties** dialog box.

Step 12 Determine if your users SMTP address is *alias@FQDN*. If it is not, you must impersonate using the user principal name (UPN). This is defined as *alias@FQDN*.

What to do next

Setting Impersonation Permissions at the Server Level , on page 20

Setting Impersonation Permissions at the Server Level

The command in the following procedure allows you to grant impersonation permissions at the server level. You can also grant permissions at the database, user, and contact levels.

Before you begin

- If you wish to only grant the service account rights to access individual Microsoft Exchange servers, replace

  ```
  Get-OrganizationConfig
  ```

  with the string

  ```
  Get-ExchangeServer -Identity ServerName
  ```

  where *ServerName* is the name of the Exchange Server.

  Example

  ```
  Add-ADPermission -Identity (Get-ExchangeServer -Identity  exchangeserver1).
  DistinguishedName -User (Get-User -Identity user | select-object).identity -ExtendedRights
  Send-As
  ```

- Verify that the SMTP address of your users is defined as alias@FQDN. If it is not, you must impersonate the user account using the User Principal Name (UPN).

Procedure

Step 1 Open the Exchange Management Shell (EMS) for command line entry.

Step 2 Run this Add-ADPermission command to add the impersonation permissions on the server.

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -AccessRights GenericAll -InheritanceType Descendents
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -AccessRights GenericAll -InheritanceType
Descendents
```

What to do next

Setting Active Directory Service Extended Permissions for the Service Account, on page 20

Setting Active Directory Service Extended Permissions for the Service Account

Before you begin

You must set these permissions on the Client Access Server (CAS) for the service account that performs the impersonation.

- If the CAS is located behind a load-balancer, grant the **ms-Exch-EPI-Impersonation** rights to the Microsoft Exchange 2007 account for all CASs behind the load-balancer.
- If your mailbox servers are located on a different machine to the CASs, grant **ms-Exch-EPI-Impersonation** rights for the Exchange 2007 account for all mailbox servers.
- You can also set these permissions by using **Active Directory Sites and Services** or the **Active Directory Users and Computers** user interfaces.

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this Add-ADPermission command in the EMS to add the impersonation permissions on the server for the identified service account (for example, Exchange 2007).

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

Step 3 Run this Add-ADPermission command in the EMS to add the impersonation permissions to the service account on each mailbox that it impersonates:

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

What to do next

Granting Send As Permissions to the Service Account and User Mailboxes, on page 21

Granting Send As Permissions to the Service Account and User Mailboxes

Follow this procedure to grant send as permissions to the service account and user mailboxes.

Note You cannot use the Microsoft Exchange Management Console (EMC) to complete this step.

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this Add-ADPermission command in the EMS to grant Send As permissions to the service account and all associated mailbox stores:

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRights Send-As
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRights Send-As
```

What to do next

Granting Impersonation Permissions to the Service Account and User Mailboxes, on page 22

Granting Impersonation Permissions to the Service Account and User Mailboxes

Follow this procedure to grant impersonation permissions to the service account and user mailboxes.

Note You cannot use the Microsoft Exchange Management Console (EMC) to complete this step.

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this **Add-ADPermission** command in the EMS to grant impersonation permissions on the service account all associated mailbox stores:

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity User | select-object) .identity -ExtendedRights Receive-As
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity EX2007 | select-object) .identity -ExtendedRights Receive-As
```

Note The IM and Presence Service only requires impersonation permissions on the account to enable it to log in to that account when it connects to the Exchange Server. This account does not typically receive mail so you do not need to be concerned about allocating space for it.

What to do next

Verifying Permissions on the Microsoft Exchange 2007 Account, on page 23

Verifying Permissions on the Microsoft Exchange 2007 Account

After you have assigned the permissions to the Exchange 2007 account, you must verify that the permissions propagate to the mailbox level and that a specified user can access the mailbox and impersonate the account of another user. On Exchange 2007, it takes some time for the permissions to propagate to mailboxes.

Procedure

Step 1 In the Exchange Management Console (EMC) on Exchange Server 2007, right-click **Active Directory Sites and Services** in the console tree.

Step 2 Point to **View**, and then choose **Show Services Node**.

Step 3 Expand the service node, for example, `Services/MS Exchange/First Organization/Admin Group/Exchange Admin Group/Servers`.

Step 4 Verify that the Client Access Server (CAS) is listed for the service node that you chose.

Step 5 View the “Properties” of each CAS, and under the Security tab, verify that:

a) Your service account is listed.

b) The permissions granted on the services account indicate (with a checked check box) that the Exchange Web Services Impersonation permission is allowed on the account.

Note If the account or the impersonation permissions do not display as advised in Step 5, you may need to recreate the service account and ensure that the required impersonation permissions are granted to the account.

Step 6 Verify that the service account (for example, Ex2007) has been granted Allow impersonationpermission on the storage group and the mailbox store to enable it to exchange personal information and to Send As and Receive-As another user account.

Step 7 You may be required to restart the Exchange Server for the changes to take effect. This has been observed during testing.

What to do next

Enable Authentication on the Exchange Virtual Directories, on page 32

Enabling Authentication on Exchange 2007 Running Windows Server 2003, on page 32

Microsoft Exchange 2010 and 2013 Configuration over Exchange Web Services

Follow these tasks when configuring access to mailboxes on Exchange 2010 and 2013 servers.

Before You Begin

Before you use Exchange Web Services (EWS) to integrate Exchange 2010 and 2013 servers with IM and Presence Service, ensure that you configure the throttle policy parameter values on the Exchange Server. These are the values that are required for the EWS calendaring integration to work with IM and Presence Service.

These are the commands and settings for Exchange Server 2010 and 2013.

Table 6: Recommended Throttle Policy Settings on Exchange Server 2010

Parameter	Recommended Configuration Value — Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] During Cisco testing, the default throttling policy value was sufficient to support 50% calendaring-enabled users. However. if you have a higher load of EWS r recommend that you increase this parameter to 100.

Table 7: Recommended Throttle Policy Settings on Exchange Server 2013 or 2016

Parameter[1]	Recommended Configuration Value — Exchange Server 2013 and 2016
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**Unlimited**
EwsRechargeRate	900000

[1] These are the only EWS parameters that can be changed in Exchange Server 2013.

Related Topics

- Exchange Server 2010
- Exchange Server 2013

Windows Security Policy Settings

IM and Presence Service integration with Microsoft Exchange supports various authentication methods including Windows Integrated authentication (NTLM).

IM and Presence Service supports both NTLMv1 and NTLMv2 Windows Integrated authentication, with NTLMv2 used as the default.

Configuring the **Lan Manager authentication level** to **Send NTLMv2 response only. Refuse LM & NTLM** on the Windows domain controller enforces NTLMv2 authentication on the domain.

Note IM and Presence Service does not support NTLMv2 session security. Message confidentiality and integrity are provided by secure http (https).

Verifying Windows Security Settings

Procedure

Step 1 On the Windows domain controller and server(s) running Exchange, choose **Start** > **Administrative Tools** > **Local Security Policy**.

Step 2 Navigate to **Security Settings** > **Local Policies** > **Security Options**.

Step 3 Choose **Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers**.

Step 4 Verify that the **Require NTLMv2 session security** check box is unchecked.

Step 5 If the **Require NTLMv2 session security** check box is checked, complete the following steps:

a) Uncheck the check box **Require NTLMv2 session security**.

b) Click **OK**.

Step 6 To apply the new security settings reboot the Windows domain controller and server(s) running Exchange.

Note The reboot is only required for servers on which a security policy configuration change was performed.

Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2010

Complete the following procedure using the Microsoft Exchange Management Shell (EMS) to set the Exchange impersonation permissions for specific users or a group of users.

These are the commands and settings for Exchange Server 2010. If you are using Exchange Server 2013, follow the steps in Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2013 or 2016 , on page 27.

Procedure

Step 1 Create the account in Active Directory.

Step 2 Open the EMS for command line entry.

Step 3 Run the New-ManagementRoleAssignment command in the EMS to grant a specified existing domain service account (for example, *Ex2010*) the permission to impersonate other user accounts:

Syntax

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

Example

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2010@contoso.com
```

Step 4 Run this New-ManagementRoleAssignment command to define the scope to which the impersonation permissions apply. In this example, the *Ex2010* account is granted the permission to impersonate all accounts on a specified Exchange Server.

Syntax

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

Example

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

Step 5 Run the New-ThrottlingPolicy command to create a new Throttling Policy with the recommended values in the table below.

Syntax

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100 -EwsPercentTimeInAD:50
-EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60 -EwsMaxSubscriptions:NULL
-EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

Example

```
New-ThrottlingPolicy -Name:IM_and_Presence_ThrottlingPolicy -EwsMaxConcurrency:100
-EwsPercentTimeInAD:50 -EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60
-EwsMaxSubscriptions:NULL -EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

Table 8: Recommended Throttle Policy Settings on Exchange Server 2010

Parameter	Recommended Configuration Value — Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] During Cisco testing, the default throttling policy value was sufficient to support 50% calendaring-enabled users. However. if you have a higher load of EWS r recommend that you increase this parameter to 100.

Note: Only available with supported Exchange SP1.

Step 6 Run the Set-ThrottlingPolicyAssociation command to associate the new Throttling Policy with the service account used in Step 2.

Syntax

```
Set-ThrottlingPolicyAssociation -Identity Username -ThrottlingPolicy Policy_Name
```

Example

```
Set-ThrottlingPolicyAssociation -Identity Ex2010 -ThrottlingPolicy
IM_and_Presence_ThrottlingPolicy
```

What to do next

Verify Permissions on the Microsoft Exchange 2010 Accounts, on page 29

Related Topics

Exchange Server 2010

Exchange Server 2013

Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2013 or 2016

Complete the following procedure using the Microsoft Exchange Management Shell (EMS) to set the Exchange impersonation permissions for specific users or a group of users.

These are the commands and settings for Exchange Server 2013 or 2016. If you are using Exchange Server 2010, follow the steps in Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2010, on page 25.

Procedure

Step 1 Create the account in Active Directory.

Step 2 Open the EMS for command line entry.

Step 3 Run the New-ManagementRoleAssignment command in the EMS to grant a specified existing domain service account (for example, *Ex2013*) the permission to impersonate other user accounts:

Syntax

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

Example

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2013@contoso.com
```

Step 4 Run this New-ManagementRoleAssignment command to define the scope to which the impersonation permissions apply. In this example, the *Ex2013*account is granted the permission to impersonate all accounts on a specified Exchange Server.

Syntax

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

Example

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

Step 5 Run the New-ThrottlingPolicy command to create a new Throttling Policy with the recommended values defined in the below table:

Syntax

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100  -EwsMaxSubscriptions:NULL
-EwsCutoffBalance 3000000 -EwsMaxBurst 300000 -EwsRechargeRate 900000
```

Example

```
New-ThrottlingPolicy -Name IMP_ThrottlingPolicy -EwsMaxConcurrency 100  -EwsMaxSubscriptions
unlimited -EwsCutoffBalance 3000000 -EwsMaxBurst 300000  -EwsRechargeRate 900000
```

Table 9: Recommended Throttle Policy Settings on Exchange Server 2013 or 2016

Parameter[1]	Recommended Configuration Value — Exchange Server 2013 and 2016
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**Unlimited**
EwsRechargeRate	900000

[1] These are the only EWS parameters that can be changed in Exchange Server 2013.

Note: Only available with supported Exchange SP1.

Step 6 Run the Set-ThrottlingPolicyAssociation command to associate the new Throttling Policy with the service account used in Step 2.

Syntax

```
Set-ThrottlingPolicyAssociation -Identity Username -ThrottlingPolicy Policy_Name
```

Example

```
Set-ThrottlingPolicyAssociation -Identity ex2013 -ThrottlingPolicy IMP_ThrottlingPolicy
```

What to do next

Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts, on page 30

Verify Permissions on the Microsoft Exchange 2010 Accounts

After you have assigned the permissions to the Exchange 2010 account, you must verify that the permissions propagate to mailbox level and that a specified user can access the mailbox and impersonate the account of another user. On Exchange 2010, it takes some time for the permissions to propagate to mailboxes.

These are the commands for Exchange Server 2010. If you are using Exchange Server 2013, follow the steps in Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts, on page 30.

Procedure

Step 1 On the Active Directory Server, verify that the Impersonation account exists.

Step 2 Open the Exchange Management Shell (EMS) for command line entry.

Step 3 On the Exchange Server verify that the service account has been granted the required Impersonation permissions:

a) Run this command in the EMS:

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

b) Ensure that the command output indicates role assignments with the Role ApplicationImpersonation for the specified account as follows:

Example Command Output

Name - - - -	Role - - -	Role AssigneeName-	Role Assig
_suImpersonate RoleAs	Application Impersonation	ex2010	User

Step 4 Verify that the management scope that applies to the service account is correct:

a) Run this command in the EMS:

```
Get-ManagementScope _suImpersonateScope
```

b) Ensure that the command output returns the impersonation account name as follows:

Example Command Output

Name - - -	Scope RestrictionType	Exclusive	Recipient Roo -
_suImpersonate Scope	ServerScope	False	User

Step 5 Verify that the ThrottlingPolicy parameters match what is defined in the below table by running this command in the EMS.

```
Get-ThrottlingPolicy -Identity Policy_Name | findstr ^EWS
```

Table 10: Recommended Throttle Policy Settings on Exchange Server 2010

Parameter	Recommended Configuration Value — Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] During Cisco testing, the default throttling policy value was sufficient to support 50% calendaring-enabled users. However. if you have a higher load of EWS r recommend that you increase this parameter to 100.

What to do next

Enable Authentication on the Exchange Virtual Directories, on page 32

Related Topics

Exchange Server 2010
Exchange Server 2013

Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts

After you have assigned the permissions to the Exchange 2013 or 2016 account, you must verify that the permissions propagate to mailbox level and that a specified user can access the mailbox and impersonate the account of another user. It takes some time for the permissions to propagate to mailboxes.

Note If you are using Exchange Server 2010, follow the steps in Verify Permissions on the Microsoft Exchange 2010 Accounts, on page 29.

Procedure

Step 1 On the Active Directory Server, verify that the Impersonation account exists.

Step 2 Open the Exchange Management Shell (EMS) for command line entry.

Step 3 On the Exchange Server verify that the service account has been granted the required Impersonation permissions:

a) Run this command in the EMS:

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

b) Ensure that the command output indicates role assignments with the Role ApplicationImpersonation for the specified account as follows:

`Example Command Output`

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonateRoleAs	ApplicationImpersonation	ex2010	User	Direct	ex2010

Step 4 Verify that the management scope that applies to the service account is correct:

a) Run this command in the EMS:

```
Get-ManagementScope _suImpersonateScope
```

b) Ensure that the command output returns the impersonation account name as follows:

`Example Command Output`

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonateScope	ServerScope	False	User	Direct	DistinguishedName

Step 5 Verify that the ThrottlingPolicy parameters match what is defined in the below table by running this command in the EMS.

```
Get-ThrottlingPolicy -Identity IMP_ThrottlingPolicy | Format-List | findstr ^Ews
```

Table 11: Recommended Throttle Policy Settings on Exchange Server 2013 or 2016

Parameter[1]	Recommended Configuration Value — Exchange Server 2013 and 2016
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**Unlimited**
EwsRechargeRate	900000

[1] These are the only EWS parameters that can be changed in Exchange Server 2013.

Step 6 Verify that they ThrottlingPolicy has been associated with the Exchange Account.

```
Get-ThrottlingPolicyAssociation -Identity ex2013
```

Enable Authentication on the Exchange Virtual Directories

Before you begin

For the Exchange Web Services (EWS) integration to work properly, Basic Authentication, Windows Integrated Authentication, or both must be enabled on the EWS virtual directory (/EWS) for Exchange Server 2007, 2010, and 2013.

Enabling Authentication on Exchange 2007 Running Windows Server 2003

Procedure

Step 1 From Administrative Tools, open **Internet Information Services** and choose the server.

Step 2 Choose **Web Sites**.

Step 3 Choose **Default Web Site**.

Step 4 Right-click **EWS** directory folder and choose **Properties**.

Step 5 Choose the **Directory Security** tab.

Step 6 Under **Authentication and access control**, click **Edit**.

Step 7 Under **Authentication Methods**, verify that the following check box is unchecked:

- **Enable anonymous access**

Step 8 Under **Authentication Methods Authenticated Access**, verify that both of the following check boxes are checked:

- **Integrated Windows authentication**
- **Basic Authentication (password is sent in clear text)**

Step 9 Click **OK**.

What to do next

Configure Certificates for Exchange Server Task Flow , on page 51

Enable Authentication on Exchange 2010, 2013 or 2016 Running Windows Server 2008

Procedure

Step 1 From Administrative Tools, open **Internet Information Services** and choose the server.

Step 2 Choose **Web Sites**.

Step 3 Choose **Default Web Site**.

Step 4 Choose **EWS**.

Step 5 Under the IIS section, choose **Authentication**.

Step 6 Verify that the following Authentication methods are enabled:

- **Anonymous Authentication**
- **Windows Authentication and/or Basic Authentication**

Step 7 Use the **Enable/Disable** link in the Actions column to configure appropriately.

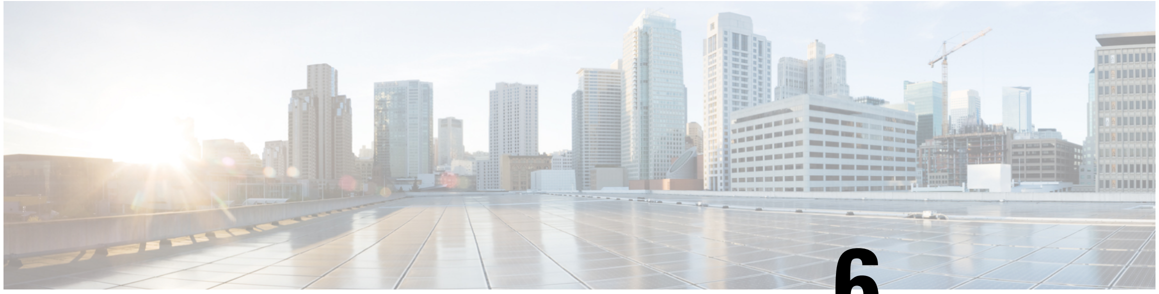
What to do next

Configure Certificates for Exchange Server Task Flow , on page 51

Related Topics

Managing Outlook Web App Virtual Directories

Enable or Disable SSL on Exchange Web Services Virtual Directories



CHAPTER 6

Configure Microsoft Exchange

Microsoft Exchange Configuration for Calendar Integration

If you are deploying an on-premise Microsoft Exchange server, complete the procedures in this chapter to configure your Microsoft Exchange for calendar integration between the IM and Presence Service and Microsoft Outlook. You can integrate the IM and Presence Service with each of the following Microsoft deployment types:

Table 12: Microsoft Exchange Configuration for Calendar Integration with the IM and Presence Service

Microsoft Exchange Deployment	Microsoft Configuration
Microsoft Exchange 2007	Microsoft Exchange 2007 Configuration Task Flow, on page 35
Microsoft Exchange 2010, 2013 or 2016	Microsoft Exchange 2010/2013/2016 Configuration Task Flow, on page 42

Note Testing is performed using the major versions of Microsoft Exchange Server. It is expected that all other cumulative updates of these major versions remain compatible. For example, when we mention Exchange 2013, it indicates that the IM and Presence service supports all Cumulative Updates (CU) released under Exchange 2013.

Microsoft Exchange 2007 Configuration Task Flow

Complete these tasks to configure a Microsoft Exchange 2007 deployment for Outlook calendar integration with the IM and Presence Service.

Procedure

	Command or Action	Purpose
Step 1	Verifying Windows Security Settings, on page 18	Verify Windows Security Settings such as your NTLM requirements.
Step 2	Configure the Exchange server to grant users the right to sign in locally: • Configuring Microsoft Exchange 2007 on Windows Server 2003, on page 19 • Configuring Microsoft Exchange 2007 on Windows Server 2008, on page 19	**Note** For Exchange impersonation to work, all Microsoft Exchange servers must be members of the Windows Authorization Access Group The service account should not be a member of any of the Exchange Administrative Groups. Exchange explicitly denies Impersonation for all accounts in those groups.
Step 3	Setting Impersonation Permissions at the Server Level , on page 20	Grant permissions at the server, database, user, and contact levels.
Step 4	Setting Active Directory Service Extended Permissions for the Service Account, on page 20	You must set permissions on the Client Access Server (CAS) for the service account that performs the impersonation.
Step 5	Granting Send As Permissions to the Service Account and User Mailboxes, on page 21	Grant send as permissions to the service account and user mailboxes.
Step 6	Granting Impersonation Permissions to the Service Account and User Mailboxes, on page 22	Grant impersonation permissions to the service account and user mailboxes.
Step 7	Verifying Permissions on the Microsoft Exchange 2007 Account, on page 23	Verify that the permissions propagate to the mailbox level and that a specified user can access the mailbox and impersonate the account of another user.
Step 8	Enabling Authentication on Exchange 2007 Running Windows Server 2003, on page 32	Enable authentication on the Exchange server.
Step 9	Configure Certificates for Exchange Server Task Flow , on page 51	Complete this task flow to configure certificates for a Microsoft Exchange deployment.

Verifying Windows Security Settings

Procedure

Step 1 On the Windows domain controller and server(s) running Exchange, choose **Start** > **Administrative Tools** > **Local Security Policy**.

Step 2 Navigate to **Security Settings** > **Local Policies** > **Security Options**.

Step 3 Choose **Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers**.

Step 4 Verify that the **Require NTLMv2 session security** check box is unchecked.

Step 5 If the **Require NTLMv2 session security** check box is checked, complete the following steps:

a) Uncheck the check box **Require NTLMv2 session security**.

b) Click **OK**.

Step 6 To apply the new security settings reboot the Windows domain controller and server(s) running Exchange.

Note The reboot is only required for servers on which a security policy configuration change was performed.

Configuring Microsoft Exchange 2007 on Windows Server 2003

Procedure

Step 1 Log in to the Exchange Server 2007 user interface using a service account that has been delegated the Exchange View Only Administrator role.

Step 2 In the left pane, under Security Settings, navigate to **Local Policies** > **User Rights Assignments**.

Step 3 In the right pane of the console, double-click **Allow Log On Locally**.

Step 4 Choose **Add User or Group** then navigate to the service account that you created and choose it.

Step 5 Choose **Check Names**, and verify that the specified user is correct.

Step 6 Click **OK**.

What to do next

Setting Impersonation Permissions at the Server Level , on page 20

Configuring Microsoft Exchange 2007 on Windows Server 2008

Procedure

Step 1 Log in to Exchange Server 2007 using a service account that has been delegated the Exchange View Only Administrator role.

Step 2 Choose Start.

Step 3 Type gpmc.msc.

Step 4 Choose Enter.

Step 5 Open the **Domain Controller Security Settings** window on the Exchange Server.

Step 6 In the left pane, under **Security Settings**, navigate to **Local Policies** > **User Rights Assignments**.

Step 7 In the right pane of the console, double-click **Allow Log On Locally**.

Step 8 Ensure that the **Define these policy settings** check box is checked.

Step 9 Choose **Add User or Group** and navigate to the service account that you previously created and choose it. Then click **OK**.

Step 10 Choose **Check Names**, and verify that the specified user is correct. Then click **OK**.

Step 11 Click **Apply** then click **OK** in the **Allow Log On Locally Properties** dialog box.

Step 12 Determine if your users SMTP address is *alias@FQDN*. If it is not, you must impersonate using the user principal name (UPN). This is defined as *alias@FQDN*.

What to do next

Setting Impersonation Permissions at the Server Level , on page 20

Setting Impersonation Permissions at the Server Level

The command in the following procedure allows you to grant impersonation permissions at the server level. You can also grant permissions at the database, user, and contact levels.

Before you begin

- If you wish to only grant the service account rights to access individual Microsoft Exchange servers, replace

  ```
  Get-OrganizationConfig
  ```

  with the string

  ```
  Get-ExchangeServer -Identity ServerName
  ```

  where *ServerName* is the name of the Exchange Server.

  ```
  Example
  ```

  ```
  Add-ADPermission -Identity (Get-ExchangeServer -Identity  exchangeserver1).
  DistinguishedName -User (Get-User -Identity user | select-object).identity -ExtendedRights
  Send-As
  ```

- Verify that the SMTP address of your users is defined as alias@FQDN. If it is not, you must impersonate the user account using the User Principal Name (UPN).

Procedure

Step 1 Open the Exchange Management Shell (EMS) for command line entry.

Step 2 Run this Add-ADPermission command to add the impersonation permissions on the server.

```
Syntax
```

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -AccessRights GenericAll -InheritanceType Descendents
```

```
Example
```

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -AccessRights GenericAll -InheritanceType
Descendents
```

What to do next

Setting Active Directory Service Extended Permissions for the Service Account, on page 20

Setting Active Directory Service Extended Permissions for the Service Account

Before you begin

You must set these permissions on the Client Access Server (CAS) for the service account that performs the impersonation.

- If the CAS is located behind a load-balancer, grant the **ms-Exch-EPI-Impersonation** rights to the Microsoft Exchange 2007 account for all CASs behind the load-balancer.
- If your mailbox servers are located on a different machine to the CASs, grant **ms-Exch-EPI-Impersonation** rights for the Exchange 2007 account for all mailbox servers.
- You can also set these permissions by using **Active Directory Sites and Services** or the **Active Directory Users and Computers** user interfaces.

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this Add-ADPermission command in the EMS to add the impersonation permissions on the server for the identified service account (for example, Exchange 2007).

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

Step 3 Run this Add-ADPermission command in the EMS to add the impersonation permissions to the service account on each mailbox that it impersonates:

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

What to do next

Granting Send As Permissions to the Service Account and User Mailboxes, on page 21

Granting Send As Permissions to the Service Account and User Mailboxes

Follow this procedure to grant send as permissions to the service account and user mailboxes.

Note You cannot use the Microsoft Exchange Management Console (EMC) to complete this step.

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this Add-ADPermission command in the EMS to grant Send As permissions to the service account and all associated mailbox stores:

```
Syntax

Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRights Send-As

Example

Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRights Send-As
```

What to do next

Granting Impersonation Permissions to the Service Account and User Mailboxes, on page 22

Granting Impersonation Permissions to the Service Account and User Mailboxes

Follow this procedure to grant impersonation permissions to the service account and user mailboxes.

Note You cannot use the Microsoft Exchange Management Console (EMC) to complete this step.

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this **Add-ADPermission** command in the EMS to grant impersonation permissions on the service account all associated mailbox stores:

```
Syntax

Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity User | select-object) .identity -ExtendedRights Receive-As

Example

Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity EX2007 | select-object) .identity -ExtendedRights Receive-As
```

Note The IM and Presence Service only requires impersonation permissions on the account to enable it to log in to that account when it connects to the Exchange Server. This account does not typically receive mail so you do not need to be concerned about allocating space for it.

What to do next

Verifying Permissions on the Microsoft Exchange 2007 Account, on page 23

Verifying Permissions on the Microsoft Exchange 2007 Account

After you have assigned the permissions to the Exchange 2007 account, you must verify that the permissions propagate to the mailbox level and that a specified user can access the mailbox and impersonate the account of another user. On Exchange 2007, it takes some time for the permissions to propagate to mailboxes.

Procedure

Step 1 In the Exchange Management Console (EMC) on Exchange Server 2007, right-click **Active Directory Sites and Services** in the console tree.

Step 2 Point to **View**, and then choose **Show Services Node**.

Step 3 Expand the service node, for example, `Services/MS Exchange/First Organization/Admin Group/Exchange Admin Group/Servers`.

Step 4 Verify that the Client Access Server (CAS) is listed for the service node that you chose.

Step 5 View the “Properties” of each CAS, and under the Security tab, verify that:

a) Your service account is listed.

b) The permissions granted on the services account indicate (with a checked check box) that the Exchange Web Services Impersonation permission is allowed on the account.

Note If the account or the impersonation permissions do not display as advised in Step 5, you may need to recreate the service account and ensure that the required impersonation permissions are granted to the account.

Step 6 Verify that the service account (for example, Ex2007) has been granted Allow impersonationpermission on the storage group and the mailbox store to enable it to exchange personal information and to Send As and Receive-As another user account.

Step 7 You may be required to restart the Exchange Server for the changes to take effect. This has been observed during testing.

What to do next

Enable Authentication on the Exchange Virtual Directories, on page 32

Enabling Authentication on Exchange 2007 Running Windows Server 2003, on page 32

Enabling Authentication on Exchange 2007 Running Windows Server 2003

Procedure

Step 1 From Administrative Tools, open **Internet Information Services** and choose the server.

Step 2 Choose **Web Sites**.

Step 3 Choose **Default Web Site**.

Step 4 Right-click **EWS** directory folder and choose **Properties**.

Step 5 Choose the **Directory Security** tab.

Step 6 Under **Authentication and access control**, click **Edit**.

Step 7 Under **Authentication Methods**, verify that the following check box is unchecked:

- **Enable anonymous access**

Step 8 Under **Authentication Methods Authenticated Access**, verify that both of the following check boxes are checked:

- **Integrated Windows authentication**
- **Basic Authentication (password is sent in clear text)**

Step 9 Click **OK**.

What to do next

Configure Certificates for Exchange Server Task Flow , on page 51

Microsoft Exchange 2010/2013/2016 Configuration Task Flow

Complete these tasks to configure a Microsoft Exchange 2010, 2013, or 2016 deployment for Outlook calendar integration with the IM and Presence Service.

Procedure

	Command or Action	Purpose
Step 1	Verify Windows Security Settings, on page 43	Verify your Windows Security Settings for Windows Integrated authentication (NTLM).

	Command or Action	Purpose
Step 2	Set Exchange permissions for your release: • Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2010, on page 25 • Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2013 or 2016 , on page 27	Set the Exchange impersonation permissions for specific users or a group of users.
Step 3	Verify permissions for your release: • Verify Permissions on the Microsoft Exchange 2010 Accounts, on page 29 • Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts, on page 30	Verify that the permissions propagate to the mailbox level and that a specified user can access the mailbox and impersonate the account of another user.
Step 4	Enable Authentication on Exchange 2010, 2013 or 2016 Running Windows Server 2008, on page 32	Basic Authentication, Windows Integrated Authentication, or both must be enabled on the EWS virtual directory (/EWS) for the Exchange Server.
Step 5	Configure Certificates for Exchange Server Task Flow , on page 51	Complete this task flow to configure certificates for a Microsoft Exchange deployment.

Verify Windows Security Settings

Procedure

Step 1 On the Windows domain controller and server(s) running Exchange, choose **Start** > **Administrative Tools** > **Local Security Policy**.

Step 2 Navigate to **Security Settings** > **Local Policies** > **Security Options**.

Step 3 Choose **Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers**.

Step 4 Verify that the **Require NTLMv2 session security** check box is unchecked.

Step 5 If the **Require NTLMv2 session security** check box is checked, complete the following steps:

a) Uncheck the check box **Require NTLMv2 session security**.

b) Click **OK**.

Step 6 To apply the new security settings reboot the Windows domain controller and server(s) running Exchange.

Note The reboot is only required for servers on which a security policy configuration change was performed.

Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2010

Complete the following procedure using the Microsoft Exchange Management Shell (EMS) to set the Exchange impersonation permissions for specific users or a group of users.

These are the commands and settings for Exchange Server 2010. If you are using Exchange Server 2013, follow the steps in Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2013 or 2016 , on page 27.

Procedure

Step 1 Create the account in Active Directory.

Step 2 Open the EMS for command line entry.

Step 3 Run the New-ManagementRoleAssignment command in the EMS to grant a specified existing domain service account (for example, *Ex2010*) the permission to impersonate other user accounts:

Syntax

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

Example

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2010@contoso.com
```

Step 4 Run this New-ManagementRoleAssignment command to define the scope to which the impersonation permissions apply. In this example, the *Ex2010* account is granted the permission to impersonate all accounts on a specified Exchange Server.

Syntax

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

Example

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

Step 5 Run the New-ThrottlingPolicy command to create a new Throttling Policy with the recommended values in the table below.

Syntax

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100 -EwsPercentTimeInAD:50
-EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60 -EwsMaxSubscriptions:NULL
-EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

Example

```
New-ThrottlingPolicy -Name:IM_and_Presence_ThrottlingPolicy -EwsMaxConcurrency:100
-EwsPercentTimeInAD:50 -EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60
-EwsMaxSubscriptions:NULL -EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

Table 13: Recommended Throttle Policy Settings on Exchange Server 2010

Parameter	Recommended Configuration Value — Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] During Cisco testing, the default throttling policy value was sufficient to support 50% calendaring-enabled users. However. if you have a higher load of E recommend that you increase this parameter to 100.

Note: Only available with supported Exchange SP1.

Step 6 Run the Set-ThrottlingPolicyAssociation command to associate the new Throttling Policy with the service account used in Step 2.

Syntax

```
Set-ThrottlingPolicyAssociation -Identity Username -ThrottlingPolicy Policy_Name
```

Example

```
Set-ThrottlingPolicyAssociation -Identity Ex2010 -ThrottlingPolicy
IM_and_Presence_ThrottlingPolicy
```

What to do next

Verify Permissions on the Microsoft Exchange 2010 Accounts, on page 29

Related Topics

Exchange Server 2010
Exchange Server 2013

Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2013 or 2016

Complete the following procedure using the Microsoft Exchange Management Shell (EMS) to set the Exchange impersonation permissions for specific users or a group of users.

These are the commands and settings for Exchange Server 2013 or 2016. If you are using Exchange Server 2010, follow the steps in Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2010, on page 25.

Procedure

Step 1 Create the account in Active Directory.

Step 2 Open the EMS for command line entry.

Step 3 Run the New-ManagementRoleAssignment command in the EMS to grant a specified existing domain service account (for example, *Ex2013*) the permission to impersonate other user accounts:

Syntax

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

Example

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2013@contoso.com
```

Step 4 Run this New-ManagementRoleAssignment command to define the scope to which the impersonation permissions apply. In this example, the *Ex2013*account is granted the permission to impersonate all accounts on a specified Exchange Server.

Syntax

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

Example

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

Step 5 Run the New-ThrottlingPolicy command to create a new Throttling Policy with the recommended values defined in the below table:

Syntax

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100  -EwsMaxSubscriptions:NULL
-EwsCutoffBalance 3000000 -EwsMaxBurst 300000 -EwsRechargeRate 900000
```

Example

```
New-ThrottlingPolicy –Name IMP_ThrottlingPolicy -EwsMaxConcurrency 100  -EwsMaxSubscriptions
unlimited –EwsCutoffBalance 3000000 -EwsMaxBurst 300000  -EwsRechargeRate 900000
```

Table 14: Recommended Throttle Policy Settings on Exchange Server 2013 or 2016

Parameter[1]	Recommended Configuration Value — Exchange Server 2013 and 2016
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**Unlimited**
EwsRechargeRate	900000

[1] These are the only EWS parameters that can be changed in Exchange Server 2013.

Note: Only available with supported Exchange SP1.

Step 6 Run the Set-ThrottlingPolicyAssociation command to associate the new Throttling Policy with the service account used in Step 2.

Syntax

```
Set-ThrottlingPolicyAssociation -Identity Username -ThrottlingPolicy Policy_Name
```

Example

```
Set-ThrottlingPolicyAssociation -Identity ex2013 -ThrottlingPolicy IMP_ThrottlingPolicy
```

What to do next

Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts, on page 30

Verify Permissions on the Microsoft Exchange 2010 Accounts

After you have assigned the permissions to the Exchange 2010 account, you must verify that the permissions propagate to mailbox level and that a specified user can access the mailbox and impersonate the account of another user. On Exchange 2010, it takes some time for the permissions to propagate to mailboxes.

These are the commands for Exchange Server 2010. If you are using Exchange Server 2013, follow the steps in Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts, on page 30.

Procedure

Step 1 On the Active Directory Server, verify that the Impersonation account exists.

Step 2 Open the Exchange Management Shell (EMS) for command line entry.

Step 3 On the Exchange Server verify that the service account has been granted the required Impersonation permissions:

a) Run this command in the EMS:

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

b) Ensure that the command output indicates role assignments with the Role ApplicationImpersonation for the specified account as follows:

Example Command Output

Name - - - -	Role - - -	Role AssigneeName-	Role Assig
_suImpersonate RoleAs	Application Impersonation	ex2010	User

Step 4 Verify that the management scope that applies to the service account is correct:

a) Run this command in the EMS:

```
Get-ManagementScope _suImpersonateScope
```

b) Ensure that the command output returns the impersonation account name as follows:

Example Command Output

Name - - -	Scope RestrictionType	Exclusive	Recipient Root -
_suImpersonate Scope	ServerScope	False	User

Step 5 Verify that the ThrottlingPolicy parameters match what is defined in the below table by running this command in the EMS.

```
Get-ThrottlingPolicy -Identity Policy_Name | findstr ^EWS
```

Table 15: Recommended Throttle Policy Settings on Exchange Server 2010

Parameter	Recommended Configuration Value — Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] During Cisco testing, the default throttling policy value was sufficient to support 50% calendaring-enabled users. However. if you have a higher load of EWS r recommend that you increase this parameter to 100.

What to do next

Enable Authentication on the Exchange Virtual Directories, on page 32

Related Topics

Exchange Server 2010
Exchange Server 2013

Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts

After you have assigned the permissions to the Exchange 2013 or 2016 account, you must verify that the permissions propagate to mailbox level and that a specified user can access the mailbox and impersonate the account of another user. It takes some time for the permissions to propagate to mailboxes.

Note If you are using Exchange Server 2010, follow the steps in Verify Permissions on the Microsoft Exchange 2010 Accounts, on page 29.

Procedure

Step 1 On the Active Directory Server, verify that the Impersonation account exists.

Step 2 Open the Exchange Management Shell (EMS) for command line entry.

Step 3 On the Exchange Server verify that the service account has been granted the required Impersonation permissions:

a) Run this command in the EMS:

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

b) Ensure that the command output indicates role assignments with the Role ApplicationImpersonation for the specified account as follows:

Example Command Output

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	User	Direct	ex2010

Step 4 Verify that the management scope that applies to the service account is correct:

a) Run this command in the EMS:

```
Get-ManagementScope _suImpersonateScope
```

b) Ensure that the command output returns the impersonation account name as follows:

Example Command Output

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

Step 5 Verify that the ThrottlingPolicy parameters match what is defined in the below table by running this command in the EMS.

```
Get-ThrottlingPolicy -Identity IMP_ThrottlingPolicy | Format-List | findstr ^Ews
```

Table 16: Recommended Throttle Policy Settings on Exchange Server 2013 or 2016

Parameter[1]	Recommended Configuration Value — Exchange Server 2013 and 2016
EwsCutoffBalance	3000000

Parameter[1]	Recommended Configuration Value — Exchange Server 2013 and 2016
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**Unlimited**
EwsRechargeRate	900000

[1] These are the only EWS parameters that can be changed in Exchange Server 2013.

Step 6 Verify that they ThrottlingPolicy has been associated with the Exchange Account.

```
Get-ThrottlingPolicyAssociation -Identity ex2013
```

Enable Authentication on Exchange 2010, 2013 or 2016 Running Windows Server 2008

Procedure

Step 1 From Administrative Tools, open **Internet Information Services** and choose the server.

Step 2 Choose **Web Sites**.

Step 3 Choose **Default Web Site**.

Step 4 Choose **EWS**.

Step 5 Under the IIS section, choose **Authentication**.

Step 6 Verify that the following Authentication methods are enabled:

- **Anonymous Authentication**
- **Windows Authentication and/or Basic Authentication**

Step 7 Use the **Enable/Disable** link in the Actions column to configure appropriately.

What to do next

Configure Certificates for Exchange Server Task Flow , on page 51

Related Topics

Managing Outlook Web App Virtual Directories
Enable or Disable SSL on Exchange Web Services Virtual Directories

SAN and Wildcard Certificate Support

The IM and Presence Service uses X.509 certificates for secure calendaring integration with Microsoft Exchange. The IM and Presence Service supports SAN and wildcard certificates, along with standard certificates.

SAN certificates allow multiple hostnames and IP addresses to be protected by a single certificate, by specifying a list of hostnames, IP addresses, or both in the X509v3 Subject Alternative Name field.

Wildcard certificates allow a domain and unlimited sub-domains to be represented by specifying an asterisk (*) in the domain name. Names may contain the wildcard character * which is considered to match any single domain name component. For example, *.a.com matches foo.a.com but not bar.foo.a.com.

Note For SAN certificates, the protected host must be contained in the list of hostnames/IP addresses in the Subject Alternative Name field. When you configure the Presence Gateway, the Presence Gateway field must exactly match the protected host listed in the Subject Alternative Name field.

Wildcards can be placed in the Common Name (CN) field for standard certificates, and in the Subject Alternative Name field for SAN certificates.

Configure Certificates for Exchange Server Task Flow

Complete these tasks to configure certificates for a Microsoft Exchange deployment.

Procedure

	Command or Action	Purpose
Step 1	Install the Certificate Authority (CA) on your version of Windows Server: • Installing a CA on Windows Server 2003, on page 52 • Installing a CA on Windows Server 2008, on page 53	Although the Certificate Authority (CA) can run on the Exchange Server, we recommend that you use a different Windows Server as a CA to provide extended security for third-party certificate exchanges
Step 2	Generate a CSR for your version of Windows Server:: • Generating a CSR – Running Windows Server 2003 , on page 54 • Generating a CSR – Running Windows Server 2008 , on page 55	You must generate a Certificate Signing Request (CSR) on the IIS Server for Exchange, which is subsequently signed by the CA Server.
Step 3	Submitting a CSR to the CA Server/Certificate Authority, on page 56	We recommend that the default SSL certificate, generated for Exchange on IIS, should use the Fully Qualified Domain Name (FQDN) of the Exchange Server and be signed by a Certificate Authority that the IM and Presence Service

	Command or Action	Purpose
		trusts. This procedure allows the CA to sign the CSR from Exchange IIS.
Step 4	Downloading a Signed Certificate, on page 57	Download a copy of the signed certificate.
Step 5	Upload the signed certificate to your version of Windows Server • Uploading a Signed Certificate – Running Windows 2003, on page 58 • Uploading a Signed Certificate – Running Windows 2008, on page 59	This procedure takes the signed CSR and uploads it onto IIS.
Step 6	Downloading a Root Certificate, on page 59	Download a root certificate from your CA server.
Step 7	Upload a Root Certificate to the IM and Presence Service Node, on page 60	Upload the root certificate into the IM and Presence Service.

Installing a CA on Windows Server 2003

Before you begin

- In order to install the CA you must first install Internet Information Services (IIS) on a Windows Server 2003 computer. IIS is not installed with the default Windows 2003 installation.
- Ensure that you have Windows Server disc 1 and SP1 discs.

Procedure

Step 1 Choose **Start** > **Control Panel** > **Add or Remove Programs**.

Step 2 In the **Add or Remove Programs** window, choose **Add/Remove Windows Components**.

Step 3 Complete the **Windows Component** wizard:

a) In the **Windows Components** window, check the check box for **Certificate Services** and click **Yes** when the warning displays about domain partnership and computer renaming constraints.

b) In the **CA Type** window, choose **Stand-alone Root CA** and click **Next** .

c) In the **CA Identifying Information** window, enter the name of the server in the Common Name field for the CA Server. If there is no DNS, type the IP address and click **Next**.

Note Remember that the CA is a third-party authority. The common name of the CA should not be the same as the common name used to generate a CSR.

d) In the **Certificate Database Settings** window, accept the default settings and click **Next**.

Step 4 Click **Yes** when you are prompted to stop Internet Information Services.

Step 5 Click **Yes** when you are prompted to enable Active Server Pages (ASP).

Step 6 Click **Finish** after the installation process completes.

What to do next

Generating a CSR – Running Windows Server 2003 , on page 54

Installing a CA on Windows Server 2008

Procedure

Step 1 Choose **Start** > **Administrative Tools** > **Server Manager**.

Step 2 In the console tree, choose **Roles**.

Step 3 Choose **Action** > **Add Roles**.

Step 4 Complete the **Add Roles** wizard:

a) In the **Before You Begin** window, ensure that you have completed all prerequisites listed and click **Next**.

b) In the **Select Server Roles** window, check the check box for **Active Directory Certificate Services** and click **Next**.

c) In the **Introduction Window** window, click **Next**.

d) In the **Select Role Services** window, check these check boxes and click **Next**.

- Certificate Authority
- Certificate Authority Web Enrollment
- Online Responder

e) In the **Specify Setup Type** window, click **Standalone**.

f) In the **Specify CA Type** window, click **Root CA**.

g) In the **Set Up Private Key** window, click **Create a new private key**.

h) In the **Configure Cryptography for CA** window, choose the default cryptographic service provider.

i) In the **Configure CA Name** window, enter a common name to identify the CA.

j) In the **Set Validity Period** window, set the validity period for the certificate generated for the CA.

Note The CA issues valid certificates only up to the expiration date that you specify.

k) In the **Configure Certificate Database** window, choose the default certificate database locations.

l) In the **Confirm Installation Selections** window, click **Install**.

m) In the **Installation Results** window, verify that the **Installation Succeeded** message displays for all components and click **Close**.

Note The Active Directory Certificate Services is now listed as one of the roles on the Server Manager.

What to do next

Generating a CSR – Running Windows Server 2008 , on page 55

Generating a CSR – Running Windows Server 2003

You must generate a Certificate Signing Request (CSR) on the IIS Server for Exchange, which is subsequently signed by the CA Server. If the Certificate has the Subject Alternative Name (SAN) field populated, it must match the Common Name (CN) of the certificate.

Before you begin

[Self-signed Certificates] Install the certificate CA service if required.

Procedure

Step 1 From Administrative Tools, open **Internet Information Services**.

a) Right-click **Default Web Site**.
b) Choose **Properties**.

Step 2 Choose the **Directory Security** tab.

Step 3 Choose **Server Certificate**.

Step 4 Click **Next** when the **Web Server Certificate** wizard displays.

Step 5 Complete the **Server Certificate** wizard:

a) In the **Server Certificate** window, choose **Create a new certificate** and click **Next**.
b) In the **Delayed or Immediate Request** window, choose **Prepare the request now, but send it later** and click **Next**.
c) In the **Name and Security Settings** window, accept the Default Web Site certificate name, choose **1024** for the bit length, and click **Next**.
d) In the **Organization Information** window, enter your Company name in the Organization field, the organizational unit of your company in the Organizational Unit field, and click **Next**
e) In the **Your Site's Common Name** window, enter the Exchange Server hostname or IP address and click **Next**.

Note The IIS certificate Common Name that you enter is used to configure the Presence Gateway on the IM and Presence Service, and must be identical to the Host (URI or IP address) you are trying to reach.

f) In the **Geographical Information** window, enter your geographical information, as follows, and click **Next**.

- Country/region
- State/province
- City/locality

g) In the **Certificate Request File Name** window, enter an appropriate filename for the certificate request, specify the path and file name where you want to save your CSR, and click **Next**.

Note Make sure that you save the CSR without any extension (.txt) and remember where you save it because you need to be able to find this CSR file after. Only use Notepad to open the file.

h) In the **Request File Summary** window, confirm that the information is correct in the **Request File Summary** window and click **Next**.

i) In the **Web Server Certificate Completion** window, click **Finish**.

What to do next

Submitting a CSR to the CA Server/Certificate Authority, on page 56

Generating a CSR – Running Windows Server 2008

You must generate a Certificate Signing Request (CSR) on the IIS Server for Exchange, which is subsequently signed by the CA Server.

Procedure

Step 1 From Administrative Tools, open the **Internet Information Services (IIS) Manager** window.

Step 2 Under Connections in the left pane of the IIS Manager, choose the Exchange Server.

Step 3 Double-click **Server Certificates**.

Step 4 Under Actions in the right pane of the IIS Manager, choose **Create Certificate Request**.

Step 5 Complete the **Request Certificate** wizard:

a) In the **Distinguished Name Properties** window, enter the following information:

- In the **Common Name** field, enter the Exchange Server hostname or IP address.
- In the **Organization** field, enter your company name
- In the **Organizational Unit** field, enter the organizational unit that your company belongs to.

b) Enter your geographic information as follows and click **Next**.

- City/locality
- State/province
- Country/region

Note The IIS certificate Common Name that you enter is used to configure the Presence Gateway on the IM and Presence Service, and must be identical to the host (URI or IP address) you are trying to reach.

c) In the **Cryptographic Service Provider Properties** window, accept the default Cryptographic service provider, choose **2048** for the bit length, and click **Next**.

d) In the **Certificate Request File Name** window, enter the appropriate filename for the certificate request and click **Next**.

Note Make sure that you save the CSR without any extension (.txt) and remember where you save it because you need to be able to find this CSR file later. Only use Notepad to open the file.

e) In the **Request File Summary** window, confirm that the information is correct and click **Next**.

f) In the **Request Certificate Completion** window, click **Finish**.

What to do next

Submitting a CSR to the CA Server/Certificate Authority, on page 56

Submitting a CSR to the CA Server/Certificate Authority

We recommend that the default SSL certificate, generated for Exchange on IIS, should use the Fully Qualified Domain Name (FQDN) of the Exchange Server and be signed by a Certificate Authority that the IM and Presence Service trusts. This procedure allows the CA to sign the CSR from Exchange IIS. Perform the following procedure on your CA Server, and configure the FQDN of the Exchange Server in the:

- Exchange certificate.
- Presence Gateway field of the Exchange Presence Gateway in **Cisco Unified CM IM and Presence Administration**.

Before you begin

Generate a CSR on IIS of the Exchange Server.

Procedure

Step 1 Copy the certificate request file to your CA Server.

Step 2 Open one of the following URLs:

- Windows 2003 or Windows 2008: http://*locall_server*/certserv

or

- Windows 2003: http://127.0.0.1/certserv
- Windows 2008: http://127.0.0.1/certsrv

Step 3 Choose **Request a certificate**.

Step 4 Choose **advanced certificate request**.

Step 5 Choose **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

Step 6 Using a text editor like Notepad, open the CSR that you generated.

Step 7 Copy all information from and including

-----BEGIN CERTIFICATE REQUEST

to and including

END CERTIFICATE REQUEST-----

Step 8 Paste the content of the CSR into the Certificate Request text box.

Step 9 (Optional) By default the Certificate Template drop-down list defaults to the Administrator template, which may or may not produce a valid signed certificate appropriate for server authentication. If you have an enterprise root CA, choose the Web Server certificate template from the Certificate Template drop-down list. The Web Server certificate template may not display, and therefore this step may not apply, if you have already modified your CA configuration.

Step 10 Click **Submit**.

Step 11 In the **Administrative Tools** window, choose **Start** > **Administrative Tools** > **Certification** > **Authority** > **CA name** > **Pending Request** to open the **Certification Authority** window. The **Certificate Authority** window displays the request you just submitted under Pending Requests.

Step 12 Right click on your request, and complete these actions:

- Navigate to **All Tasks**.
- Choose **Issue**.

Step 13 Choose **Issued certificates** and verify that your certificate has been issued.

What to do next

Downloading a Signed Certificate, on page 57

Downloading a Signed Certificate

Before you begin

[Self-signed Certificates] Submit the Certificate signing request (CSR) to the CA server.

[Third-Party Certificates] Request the CSR from your Certificate Authority.

Procedure

Step 1 In Administrative Tools, open the Certification Authority. The Certificate Request that you issued displays in the Issued Requests area.

Step 2 Right click the request and choose **Open**.

Step 3 Choose the **Details** tab.

Step 4 Choose **Copy to File**.

Step 5 When the **Certificate Export** wizard displays, click **Next**.

Step 6 Complete the **Certificate Export** wizard:

a) In the **Export File Format** window, choose **Base-64 encoded X.509** and click **Next**.

b) In the **File to Export** window, enter the location where you want to store the certificate, use cert.cer for the certificate name, and choose `c:\cert.cer`.

c) In the **Certificate Export Wizard Completion** window, review the summary information, verify that the export was successful, then click **Finish**.

Step 7 Copy or FTP the cert.cer to the computer that you use to administer the IM and Presence Service.

What to do next

Upload of Signed Certificate onto Exchange IIS, on page 84

Upload a signed certificate for your server type:

- Uploading a Signed Certificate – Running Windows 2003, on page 58

- Uploading a Signed Certificate – Running Windows 2008, on page 59

Uploading a Signed Certificate – Running Windows 2003

This procedure takes the signed CSR and uploads it onto IIS. To upload the signed certificate, perform the following steps on the computer that you use to administer the IM and Presence Service.

Before you begin

[Self-signed Certificates] Download the signed certificate.

[Third-party Certificates] Your Certificate Authority provides you with the signed certificate.

Procedure

Step 1 From Administrative Tools, open **Internet Information Services**.

Step 2 Complete the following steps in the **Internet Information Services** window:

a) Right-click **Default Web Site**.
b) Choose **Properties**.

Step 3 In the **Default Web Site Properties** window, complete the following steps:

a) Choose the **Directory Security** tab.
b) Choose **Server Certificate**.

Step 4 When the **Web Server Certificate** wizard window displays, click **Next** .

Step 5 Complete the **Web Server Certificate** wizard:

a) In the **Pending Certificate Request** window, choose **Process the pending request and install the certificate** and click **Next**.
b) In the **Process a Pending Request** window, click **Browse** to locate your certificate and navigate to the correct path and filename.
c) In the **SSL Port** window, enter 443 for the SSL port and click **Next**.
d) In the **Web Server Certificate Completion** window, click **Finish**.

Tip

If your certificate is not in the trusted certificates store, the signed CSR is not trusted. To establish trust, complete these actions:

- Under the **Directory Security** tab, click **View Certificate**.
- Choose **Details** > **Highlight root certificate**, and click **View**.
- Choose the **Details** tab for the root certificate and install the certificate.

What to do next

Downloading a Root Certificate, on page 59

Uploading a Signed Certificate – Running Windows 2008

This procedure takes the signed CSR and uploads it onto IIS. To upload the signed certificate, perform the following step on the computer that you use to administer the IM and Presence Service.

Before you begin

[Self-signed Certificates] Download the signed certificate.

[Third-party Certificates] Your Certificate Authority provides the signed certificate.

Procedure

Step 1 From Administrative Tools, open the **Internet Information Services (IIS) Manager** window.

Step 2 Under Connections in the left pane of the IIS Manager, choose the Exchange Server.

Step 3 Double-click **Server Certificates**.

Step 4 Under Actions in the right pane of the IIS Manager, choose **Complete Certificate Request**.

Step 5 In the **Specify Certificate Authority Response** window, complete these actions:

a) To locate your certificate, choose the ellipsis [...].
b) Navigate to the correct path and filename.
c) Enter a user-friendly name for your certificate.
d) Click **Ok**. The certificate that you completed displays in the certificate list.

Step 6 In the **Internet Information Services** window, complete the following steps to bind the certificate:

a) Choose **Default Web Site**.
b) Under Actions in the right pane of the IIS Manager, choose **Bindings**.

Step 7 Complete the following steps in the **Site Bindings** window:

a) Choose **https**.
b) Choose **Edit**.

Step 8 In the **Edit Site Binding** window, complete the following steps :

a) Choose the certificate that you just created from the SSL certificate drop-down list. The name that you applied to the certificate displays.
b) Click **Ok**.

What to do next

Downloading a Root Certificate, on page 59

Downloading a Root Certificate

Before you begin

Upload the Signed Certificate onto Exchange IIS.

Procedure

Step 1 Log in to your CA Server user interface and open a web browser.

Step 2 Open the URL specific to your Windows platform type:

a) Windows Server 2003 – http://127.0.0.1/certserv

b) Windows Server 2008 – https://127.0.0.1/certsrv

Step 3 Choose **Download a CA certificate, certificate chain, or CRL**.

Step 4 For the Encoding Method, choose **Base 64**.

Step 5 Click **Download CA Certificate**.

Step 6 Save the certificate, **certnew.cer**, to the local disk.

Tip

If you do not know the Subject Common Name (CN) of the root certificate, you can use an external certificate management tool to find this information. On a Windows operating system, right-click the certificate file with a .cer extension and open the certificate properties.

What to do next

Upload a Root Certificate to the IM and Presence Service Node, on page 60

Upload a Root Certificate to the IM and Presence Service Node

Before you begin

- [Self-signed Certificates] Download the root certificate.
- [Third-party Certificates] Request the root certificate from your Certificate Authority. If you have a third-party CA-signed Exchange server certificate, note that you must upload all CA certificates in the certificate chain to the IM and Presence Service as a CiscoUnified Presence Trust certificate (cup-trust).

Procedure

Step 1 Use the Certificate Import Tool in **Cisco Unified CM IM and Presence Administration** to upload the certificate:

Upload the certificate via:	Actions
Certificate Import Tool in **Cisco Unified CM IM and Presence Administration**. The Certificate Import tool simplifies the process of installing trust certificates on the IM and Presence Service and is the primary method for certificate exchange. The tool allows you to specify the host and port of the Exchange server and attempts to download the certificate chain from the server. Once approved, the tool automatically installs missing certificates. **Note** This procedure describes one way to access and configure the Certificate Import Tool in **Cisco Unified CM IM and Presence Administration**. You can also view a customized version of the Certificate Import Tool in **Cisco Unified Presence Administration** when you configure the Exchange Presence Gateway for a specific type of calendaring integration (Log in to **Cisco Unified CM IM and Presence Administration** and choose **Presence** > **Gateways**).	**a.** Log in to the **Cisco Unified CM IM and Presence Admi** **b.** Choose **System** > **Security** > **Certificate Import Tool**. **c.** Choose **IM and Presence(IM/P) Trust** as the Certificate to install the certificates. This stores the Presence Engine t Exchange integration. **d.** Enter one of these values to connect with the Exchange Se • IP address • Hostname • FQDN The value that you enter in this Peer Server field must exa hostname or FQDN of the Exchange Server. **e.** Enter the port that is used to communicate with the Excha match the available port on the Exchange Server. **f.** Click **Submit**. After the tool finishes, it reports these state • Peer Server Reachability Status — indicates whether Service can reach (ping) the Exchange Server. See Trou Connection Status, on page 93. • SSL Connection/Certificate Verification Status — inc Certificate Import Tool succeeded in downloading ce peer server and whether or not a secure connection ha the IM and Presence Service and the remote server. S Connection Certificate Status , on page 94.

Step 2 If the Certificate Import Tool indicates that certificates are missing (typically the CA certificate is missing on Microsoft servers), manually upload the CA certificate(s) using the **Cisco Unified OS Admin Certificate Management** window.

Upload the certificate via:	Actions
Cisco Unified IM and Presence Operating System Administration If the Exchange Server does not provide the CA certificates during the SSL/TLS handshake, you cannot use the Certificate Import Tool to import those certificates. In this case, you must manually import the missing certificates using the Certificate Management tool in (Log in to **Cisco Unified IM and Presence Operating System Administration**. Choose **Security** > **Certificate Management**).	**a.** Copy or FTP the **certnew.cer** certificate file to the computer th your IM and Presence Service node. **b.** Log in to the **Cisco Unified IM and Presence Operating Sy** user interface. **c.** Choose **Security** > **Certificate Management**. **d.** In the **Certificate List** window, choose **Upload Certificate/C** **e.** Complete these actions when the **Upload Certificate/Certific** opens: • From the Certificate Name drop-down list, choose **cup-t** • Enter the root certificate name without any extension. **f.** Click **Browse** and choose **certnew.cer**. **g.** Click **Upload File**.

Step 3 Return to the Certificate Import Tool (Step 1, on page 60) and verify that all status tests succeed.

Step 4 Restart the CiscoPresence Engine and SIP Proxy service after you upload all Exchange trust certificates. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Feature Services**.

Tips

The IM and Presence Service allows you to upload Exchange Server trust certificates with or without a Subject Common Name (CN).

What to do next

Configure the IM and Presence Service, on page 67

CHAPTER 7

Configure Microsoft Office 365

Microsoft Office 365 Calendar Integration

You can configure the IM and Presence Service to integrate with a hosted Office 365 server for Microsoft Outlook calendaring integration. When this feature is configured, the IM and Presence Service pulls user calendar information from the Office 365-hosted Microsoft Outlook and displays it as a part of an IM and Presence user's presence status. If the user's Outlook indicates that the user is in a meeting that status displays in the user's presence status.

This integration has been tested successfully with 15,000 IM and Presence users system, where 5,000 users have a meeting at the top of the hour.

Microsoft Office 365 Calendar Integration Task Flow

Complete these tasks to configure your Microsoft Office 365 deployment for calendar integration between the IM and Presence Service and Microsoft Outlook.

Procedure

	Command or Action	Purpose
Step 1	Configure Office 365 Permissions for Calendar Integration, on page 64	Configure the Office 365 server with impersonation permissions to allow IM and Presence users to pull calendar information from Microsoft Outlook.
Step 2	Upload Microsoft Certificates to IM and Presence Service, on page 64	Download the Microsoft certificates that will be required for integration with the IM and Presence Service.

Configure Office 365 Permissions for Calendar Integration

Use this procedure on the Office 365 server to configure permissions for IM and Presence calendar integration. To integrate with the IM and Presence Service, you must assign the **ApplicationImpersonation** admin role for Discovery Management.

Before you begin

This procedure assumes that you have already set up your Office365 deployment. For Office365 configuration, see your Microsoft documentation.

Procedure

Step 1 Log in to Office 365.

Step 2 Click the **Admin** icon

Step 3 In the left navigation bar, select the **Admin Center** tab (bottom left) and click **Exchange**.

Step 4 Under **Permissions** select **Admin roles**.

Step 5 Select **Discovery Management**.

Step 6 Click the Pencil icon to edit the role assignments.

Step 7 Add the **ApplicationImpersonation** role by doing the following:

a) Under **Roles** click +.
b) Select **ApplicationImpersonation** and click **Add**.
c) Click **OK**.

Step 8 Assign a user as a member of the ApplicationImpersonation role:

a) Under **Members** click +.
b) Select the user account that you want to add and click **Add**.
c) Click **OK**.

Step 9 Click **Save**.

What to do next

Upload Microsoft Certificates to IM and Presence Service, on page 64

Upload Microsoft Certificates to IM and Presence Service

For the IM and Presence Service and the Office 365 deployment to communicate, you must install the Microsoft certificates on the IM and Presence Service.

Procedure

Step 1 Download an Office 365 root certificate, and intermediate certificate:

- The following site lists all of the root and intermediate certificates that Office 365 supports: https://support.office.com/en-us/article/office-365-certificate-chains-0c03e6b3-e73f-4316-9e2b-bf4091ae96bb

Step 2 Upload all certificates to the **cup-trust** and **tomcat-trust** stores on the IM and Presence Service.

Note For additional details on certificates with the IM and Presence Service, refer to the "Security Configuration on IM and Presence Service" chapter of the *Configuration and Administration Guide for IM and Presence Service*.

What to do next

Configure the IM and Presence Service, on page 67

CHAPTER 8

Configure the IM and Presence Service

IM and Presence Calendar Integration Task Flow

Complete these tasks on the IM and Presence Service to set up calendar integration with Microsoft Outlook for either of the following Microsoft deployments:

- An on-premise Microsoft Exchange server
- A hosted Microsoft Office 365 server

Procedure

	Command or Action	Purpose
Step 1	Configure a Presence Gateway, on page 68	On the IM and Presence server configure the Exchange server or Office 365 server as a Presence Gateway.
Step 2	Configure Pull Interval for Office 365 Integration, on page 70	(Office 365 only) Configure the interval schedule by which the IM and Presence Service pulls calendar information from Office 365. The default value is 60 minutes.
Step 3	Configure Service Parameters for Exchange Integration , on page 70	(Exchange only) Configure optional service parameters that outline the calendar sync interaction with the Microsoft Exchange server.
Step 4	Restart the Cisco Presence Engine, on page 72	If you edited any service parameters, restart the Cisco Presence Engine service.
Step 5	Enable calendaring for users using one of the following procedures: • Enable Calendaring for LDAP Synchronized Users, on page 72 • Enable Calendar Integrations by Bulk, on page 74	Select the procedure that fits your needs: • If you have not yet completed an LDAP sync, enable calendaring via the LDAP sync.

	Command or Action	Purpose
	• Enable Calendar Integration for a User, on page 74	• Otherwise, use the Bulk Administration Tool to configure calendaring for a large number of users. • Or enable the feature on a user by user basis.

Configure a Presence Gateway

Use this procedure to configure a Presence Gateway to set up calendar integration with Microsoft Outlook. You can assign either a Microsoft Exchange server or an Office 365 server as the Presence Gateway.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Gateways**.

Step 2 Click **Add New**.

Step 3 From the **Presence Gateway Type** field, choose one of the following options:

a) Select **Exchange - - EWS Server**, if you are integrating with an on-premise Exchange server.

b) Select **Office 365 Server**, if you are integrating with a hosted Office 365 server.

If you choose **Office 365 Server**, then you need to choose an **Authentication Type** from the drop-down list, by choosing either **Basic** or **OAuth**.

Note • The fields **Application (client) ID**, **Directory (tenant) ID**, and **Client Secret** are applicable only if you choose the **Authentication Type** as **OAuth.**

See section Office 365 Pre-Configuration for Authentication type OAuth, on page 69 to configure the fields **Application (client) ID**, **Directory (tenant) ID**, **Client Secret**, to set application permissions and grant admin consent.

Note This note is applicable from release 12.5(1)SU8 onwards.

The **Basic** Authentication Type for Office 365 server is deprecated. Please re-configure the Authentication Type with the default option **OAuth** from 12.5(1)SU8 onwards.

Step 4 In the **Description** field, enter a description that will help you to distinguish the presence gateway instance.

Step 5 In the **Presence Gateway** field, enter the fully qualified domain name or IP address of the Presence Gateway server. This value must match the server address that is displayed in the **Subject Common Name (CN)** or **Subject Alternate Name** field of the server certificate.

Step 6 In the **Account Name** field, enter the account name to access the server.

Step 7 Enter the password that the account uses to access the server in both the **Account Password** and **Confirm Password** fields.

Step 8 In the **HTTP/HTTPS Proxy URL** field, assign HTTP/HTTPS Proxy server details, if the **Presence Gateway Type** is **Office 365 Server** and IM and Presence Service doesn't have access to Office 365Server.

Step 9 In the **HTTP/HTTPS Proxy Username** field, enter the user name to access the HTTP/HTTPS proxy server.

Step 10 In the **HTTP/HTTPS Proxy Password** field, enter the password for the user name provided for HTTP/HTTPS proxy server.

Step 11 Complete the remaining fields in the **Presence Gateway Settings** window. For more information on the fields and settings, see the online help.

Step 12 Click **Save**.

What to do next

You can configure optional parameters for your Microsoft integration type:

- Configure Pull Interval for Office 365 Integration, on page 70
- Configure Service Parameters for Exchange Integration , on page 70

Office 365 Pre-Configuration for Authentication type OAuth

Use this procedure to configure the Presence Gateway Authentication Type as OAuth.

You need to follow the steps mentioned in the procedure to fetch the Application (client) ID, Directory (tenant) ID and Client Secret, to set application permission and to grant admin consent from Microsoft Azure portal.

Procedure

Step 1 Log in to Microsoft Azure portal: https://portal.azure.com.

Step 2 Register the new Application and fetch **Application (client) ID** and **Directory (tenant) ID** by following the steps available at: https://docs.microsoft.com/en-gb/azure/active-directory/develop/quickstart-register-app#register-a-new-application-using-the-azure-portal.

Step 3 To create the **Client Secret**, under **Manage**, click **Certificates & Secrets** > **New Client Secret**.

Note If you choose **Presence Gateway Type** as **Office 365 Server** and **Authentication Type** as **OAuth**, use the same values to configure the Application (client) ID, Directory (tenant) ID and Client Secret fields on IM and Presence during the Presence Gateway configuration.

Step 4 Click **Manage** > **API Permissions** > **Add a permission**, and choose **Office 365 Exchange Online** under **APIs my organization uses**.

Step 5 To add an application permission, select **Application permissions** > **Permission**, check the check box **full_access_as_app** and click **Add permissions**.

Step 6 To grant admin consent, click **Manage** > **API permissions**.

Step 7 Under **Grant consent**, click **Grant admin consent for "registered Azure Active Directory"** and choose **Yes**.

Step 8 Check if there is a green tick mark against **Status** column for **full_access_as_app** permission.

Configure Pull Interval for Office 365 Integration

Use this procedure to configure the interval period following which the IM and Presence Service pulls calendar information from Office 365.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down, choose the IM and Presence publisher node.

Step 3 From the **Service** drop-down, choose **Cisco Presence Engine**.

Step 4 Configure an interval, in minutes for the **Office 365 Calendar Information Pull Interval** service parameter. The default is 60 minutes.

Step 5 Click **Save**.

Note The IM and Presence Service pulls information from Office 365 at scheduled intervals as specified by the **Office 365 Calendar Information Pull Interval** service parameter (default value is 60 minutes). However, there is no mechanism for pushing information from Office 365 to the IM and Presence Service. As a result, if a non-scheduled Presence update occurs in Office 365 between scheduled pulls (for example, an ad hoc meeting), the results do not register with the IM and Presence Service until after the next scheduled pull.

What to do next

Enable calendaring for IM and Presence Service users. To enable the feature for a large number of users at once, you can use either an LDAP sync for users whom are synced from an external LDAP directory, or the Bulk Administration Tool for non-LDAP users. Otherwise, you can enable the feature for users on an individual basis.

- Enable Calendaring for LDAP Synchronized Users, on page 72
- Enable Calendar Integrations by Bulk, on page 74
- Enable Calendar Integration for a User, on page 74

Configure Service Parameters for Exchange Integration

Use this optional procedure to configure optional service parameters for Outlook calendar integration with a Microsoft Exchange server. The default values may be sufficient for many parameters.

Procedure

Step 1 From Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down, choose the IM and Presence publisher node.

Step 3 From the **Service** drop-down, choose **Cisco Presence Engine**.

Step 4 Under **Calendaring Configuration**, configure values for the following parameters:

Table 17: Service Parameters for Exchange Integration

Service Parameter	Description
Microsoft Exchange Notification Port	The port number that the Presence Engine will listen on for incoming notifications from the Exchange server. UDP is used for WebDav and TCP is used for EWS (Exchange Web Services). Possible values are 1024-65535 with a default value of 50020.
Calendar Spread (seconds)	This parameter specifies the range of duration in seconds. Each user will be assigned an offset duration by a hash. The duration will determine the number of seconds after the top-of-minute that meeting transitions will be sent. The duration can be shortened for smaller numbers of users (approx. users / 100 = seconds). It is used for WebDav and EWS (Exchange Web Services). The range of values is 0-59 with a default value of 50 seconds.
Exchange Timeout (seconds)	This parameter specifies the duration, in seconds, before a request made to an Exchange server times out. This change requires a restart of the Cisco Presence Engine. The range of possible values is 1 - 20 with a default value of 3 seconds.
Exchange Queue	This parameter specifies the maximum length of the Exchange request queue. If a request is made and the queue length is exceeded, the request will fail and a recovery procedure will be initiated. This change requires a restart of the Cisco Presence Engine. Possible values are 1-5000 with a default value of 2200.
Exchange Threads	This parameter specifies the number of threads that are used to service Exchange requests. You can increase this value if there are a large number of users (for example, 5000) or if some Exchange transactions take longer than 3 seconds. If calendar integration is disabled, set this parameter to 1. This change requires a restart of the Cisco Presence Engine. Possible values are 1-100 with a default value of 60.
EWS Status Frequency (minutes)	This parameter specifies how often notification messages are sent from the Exchange server when EWS (Exchange Web Services) is used. The duration is in minutes. Possible values are 10 - 1440 with a default value of 60.

Step 5 Click **Save**.

What to do next

Restart the Cisco Presence Engine, on page 72

Restart the Cisco Presence Engine

If you changed the values for any of the Calendaring Configuration service parameters, restart the Cisco Presence Engine service.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**.

Step 2 From the **Server** drop-down, choose the IM and Presence server and click **Go**.

Step 3 Under **IM and Presence Services**, select **Cisco Presence Engine** and click **Restart**.

What to do next

Enable calendaring for IM and Presence Service users. To enable the feature for a large number of users at once, you can use an LDAP sync if users are synced from an external LDAP directory, or the Bulk Administration Tool for non-LDAP users. Otherwise, you can enable the feature for users on an individual basis.

- Enable Calendaring for LDAP Synchronized Users, on page 72
- Enable Calendar Integrations by Bulk, on page 74
- Enable Calendar Integration for a User, on page 74

Enable Calendaring for LDAP Synchronized Users

Complete these tasks to enable calendaring via the initial LDAP directory sync. You can use the initial LDAP sync to enable calendaring for users synced from the LDAP directory.

Procedure

	Command or Action	Purpose
Step 1	Add Calendar Integration to a Feature Group Template, on page 72	Assign calendaring to a feature group template.
Step 2	Add Feature Group Template to LDAP Sync, on page 73	Assign your calendaring-enabled feature group template to an LDAP directory sync and complete a sync.

Add Calendar Integration to a Feature Group Template

Use this procedure to assign Microsoft Outlook calendaring integration to a feature group template. You can use the template to configure Outlook calendar integration for all users synchronized from an LDAP directory

Note You can only add or edit feature group template settings for an LDAP directory that has not yet been synced. If the directory is already synced, use Enable Calendar Integrations by Bulk, on page 74 instead.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Phone/Add** > **Feature Group Template**.

Step 2 Complete one of the following steps:

- Click **Add New** to create a new template.
- Click **Find** and select an existing template

Step 3 Check the **Enable User for Unified CM IM and Presence** check box

Step 4 Check the **Include meeting information in Presence** check box

Step 5 Complete the remaining fields in the **Feature Group Template** configuration window. For help with the fields and their settings, see the online help.

Step 6 Click **Save**.

What to do next

Add Feature Group Template to LDAP Sync, on page 73

Add Feature Group Template to LDAP Sync

Use this procedure to assign the calendaring-enabled feature group template that you just created to an LDAP Directory sync. This will allow you to enable Outlook calendar integration for all users synced from this LDAP Directory.

Note You can only add a feature group template to an LDAP directory that has not yet been synced. If the directory is already synced, use Enable Calendar Integrations by Bulk, on page 74 instead.

Before you begin

Add Calendar Integration to a Feature Group Template, on page 72

Procedure

Step 1 From Cisco Unified CM Administration choose **System** > **LDAP** > **LDAP Directory**.

Step 2 Click **Find** and select an existing LDAP Directory.

Step 3 From the **Feature Group Template** drop-down menu, select the calendaring-enabled feature group template that you created in the previous task.

Step 4 Complete the remaining fields in the **LDAP Directory** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

Step 6 Click **Perform Full Sync Now**.

Enable Calendar Integrations by Bulk

Use Bulk Administration to enable calendar integration for a large number of users in a single operation.

Procedure

Step 1 On a Cisco Unified Communications Manager node, log in to the **Cisco Unified CM Administration** user interface.

Step 2 Enabling calendar integrations in bulk can be performed from the following windows:

a) **Bulk Administration** > **Users** > **Insert Users**.
b) **Bulk Administration** > **Users** > **Update Users** > **Query**.
c) **Bulk Administration** > **Users** > **Update Users** > **Custom File**.

Note For information on the different types of update options, refer to the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Step 3 For all end users for whom you want to enable calendar integration, make sure that the following end user configuration options are checked:

- **Enable User for Unified CM IM and Presence**
- **Include meeting information in Presence**

Step 4 If you are updating from a csv file, in the appropriate Users area, choose a File Name.

Note Click **View Sample File** for the correct file format.

Step 5 Click **Run Immediately** or **Run Later**.

Step 6 Click **Submit**.

Enable Calendar Integration for a User

Use this procedure to enable calendar integration for an IM and Presence Service user.

Procedure

Step 1 Log in to the **Cisco Unified CM Administration** user interface.

Step 2 Choose **User Management** > **End User**.

Step 3 Click **Find** and select an end user.

Step 4 Check the **Enable User for Unified CM IM and Presence** check box.

Step 5 Check the **Include meeting information in presence** check box.

Step 6 Click **Save**.

CHAPTER 9

Configure IM and Presence Service for Calendar Integration

Configure a Presence Gateway for Microsoft Exchange Integration

You must configure an Exchange Server (Microsoft Outlook) as a Presence Gateway for calendaring information exchange. The Exchange gateway enables the IM and Presence Service node to reflect the availability information of the user on a per-user basis.

When you configure the Presence Gateway, you can use one of the following values to connect the Exchange Server:

- FQDN (resolvable by DNS)
- IP address

When configuring your Exchange Web Services (EWS) Presence Gateway for Exchange integration through the **Cisco Unified CM IM and Presence Administration** user interface, note the following:

- You can add, update, or delete *one or more* EWS servers with no maximum limit. However, the Troubleshooter on the **Presence Gateway Configuration** window is designed to only verify and report status of the first 10 EWS servers that you configure.
- EWS Server gateways share the Impersonation Account credentials (Account Name and Password) that you configure for the first EWS Server Gateway. If you change the credentials for one EWS Server Gateway, the credentials change accordingly on all of the configured EWS gateways.

- You must restart the Cisco Presence Engine after you add, update, or delete one or more EWS servers for your configuration changes to take effect. If you add multiple EWS servers one after another, you can restart the Cisco Presence Engine once to effect all your changes simultaneously.

Note

- For SAN certificates, the protected host must be contained in the list of hostnames/IP addresses in the Subject Alternative Name field.
- When you are configuring the Presence Gateway, the Presence Gateway field must exactly match the protected host listed in the Subject Alternative Name field.

Configure Exchange 2007, 2010, or 2013 as a Presence Gateway over Exchange Web Services

Before you begin

Before you configure a Presence Gateway, you must upload a valid certificate chain to the IM and Presence Service.

If the connection to the Microsoft Exchanger server is over IPv6, ensure that the enterprise parameter is configured for IPv6 and that Eth0 is set for IPv6 on each IM and Presence Service node in the deployment. For information about configuring IPv6 on IM and Presence Service, see the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface.

Step 2 Choose **Presence** > **Gateways**.

Step 3 Click **Add New**.

Step 4 Choose **Exchange -- EWS Server** for the Presence Gateway Type.

For configuration changes to take effect, you must restart the Cisco Presence Engine after you add, update, or delete one or more EWS servers. If you add multiple EWS servers one after another, you can restart the Cisco Presence Engine once to effect all your changes simultaneously.

Step 5 Enter a meaningful description in the **Description** field that helps you to distinguish between Presence Gateway instances when you have configured more than one type of gateway.

Step 6 For the Presence Gateway field, enter the server location for the Presence Gateway and ensure that it matches the Subject Common Name (CN) or is present in the Subject Alternative Name field of the Exchange Server certificate. One of these values must be used to connect with the Exchange Server:

- FQDN
- IP address

To configure a Presence Gateway for use with a Wildcard Certificate, the node location value that you specify must be part of the subdomain that is protected by the Wildcard Certificate. For example, if a Wildcard Certificate protects the subdomain `*.imp.cisco.com`, you must enter a node value of *`server_name`*`.imp.cisco.com` in the Presence Gateway field.

Note If you enter a FQDN, it must match the Subject Common Name (CN) or match one of the protected hosts in the Subject Alternative Name field on the Exchange Server leaf certificate in the certificate chain. The FQDN must resolve to the address that services the request and uses the certificate.

For IPv6, the IPv6 address you enter must match the value that is entered in the SAN field of the Exchange Server certificate.

Step 7 Enter the name of the Impersonation account that the IM and Presence Service uses to connect to the Exchange Server, either in the form of a User Principal Name (for example, user@domain), or a Down-Level Logon Name (for example, domain\user).

Step 8 Enter the Exchange Account Password required for the IM and Presence Service to connect to the Exchange Server. Enter the password again to confirm it. This value must match the Account Password of the previously configured account on the Exchange Server.

Step 9 Enter the port that is used to connect with the Exchange Server. The IM and Presence Service integration with Exchange occurs over a secure HTTP connection. Cisco recommends that you use port 443 (default port) and not change to other ports.

Step 10 Click **Save**.

Step 11 Confirm the Exchange Server status is showing green for:

- **Exchange Reachability (pingable)**
- **Exchange SSL Connection/Certification Verification**

What to do next

After you configure the Exchange Presence Gateway, verify the following:

- Did the connection between the IM and Presence Service and the Exchange Server succeed? The Exchange Server Status area in the **Presence Gateway Configuration** window reports the connection status. If you need to take corrective action, see Troubleshooting Exchange Server Connection Status, on page 93.

- Is the status of the Exchange SSL certificate chain correct (verified)? The Exchange Server Status area in the **Presence Gateway Configuration** window indicates if there is a certificate Subject CN mismatch. If you need to take corrective action, see Troubleshooting SSL Connection Certificate Status , on page 94.

SAN and Wildcard Certificate Support

The IM and Presence Service uses X.509 certificates for secure calendaring integration with Microsoft Exchange. The IM and Presence Service supports SAN and wildcard certificates, along with standard certificates.

SAN certificates allow multiple hostnames and IP addresses to be protected by a single certificate, by specifying a list of hostnames, IP addresses, or both in the X509v3 Subject Alternative Name field.

Wildcard certificates allow a domain and unlimited sub-domains to be represented by specifying an asterisk (*) in the domain name. Names may contain the wildcard character * which is considered to match any single domain name component. For example, *.a.com matches foo.a.com but not bar.foo.a.com.

Note For SAN certificates, the protected host must be contained in the list of hostnames/IP addresses in the Subject Alternative Name field. When you configure the Presence Gateway, the Presence Gateway field must exactly match the protected host listed in the Subject Alternative Name field.

Wildcards can be placed in the Common Name (CN) field for standard certificates, and in the Subject Alternative Name field for SAN certificates.

Configure Secure Certificate Exchange Between the IM and Presence Service and Microsoft Exchange

How to Install the Certificate Authority Service

Although the Certificate Authority (CA) can run on the Exchange Server, we recommend that you use a different Windows Server as a CA to provide extended security for third-party certificate exchanges.

- Installing a CA on Windows Server 2003, on page 52
- Installing a CA on Windows Server 2008, on page 53

Installing a CA on Windows Server 2003

Before you begin

- In order to install the CA you must first install Internet Information Services (IIS) on a Windows Server 2003 computer. IIS is not installed with the default Windows 2003 installation.
- Ensure that you have Windows Server disc 1 and SP1 discs.

Procedure

Step 1 Choose **Start** > **Control Panel** > **Add or Remove Programs**.

Step 2 In the **Add or Remove Programs** window, choose **Add/Remove Windows Components**.

Step 3 Complete the **Windows Component** wizard:

a) In the **Windows Components** window, check the check box for **Certificate Services** and click **Yes** when the warning displays about domain partnership and computer renaming constraints.

b) In the **CA Type** window, choose **Stand-alone Root CA** and click **Next** .

c) In the **CA Identifying Information** window, enter the name of the server in the Common Name field for the CA Server. If there is no DNS, type the IP address and click **Next**.

Note Remember that the CA is a third-party authority. The common name of the CA should not be the same as the common name used to generate a CSR.

d) In the **Certificate Database Settings** window, accept the default settings and click **Next**.

Step 4 Click **Yes** when you are prompted to stop Internet Information Services.

Step 5 Click **Yes** when you are prompted to enable Active Server Pages (ASP).

Step 6 Click **Finish** after the installation process completes.

What to do next

Generating a CSR – Running Windows Server 2003 , on page 54

Installing a CA on Windows Server 2008

Procedure

Step 1 Choose **Start** > **Administrative Tools** > **Server Manager**.

Step 2 In the console tree, choose **Roles**.

Step 3 Choose **Action** > **Add Roles**.

Step 4 Complete the **Add Roles** wizard:

a) In the **Before You Begin** window, ensure that you have completed all prerequisites listed and click **Next**.
b) In the **Select Server Roles** window, check the check box for **Active Directory Certificate Services** and click **Next**.
c) In the **Introduction Window** window, click **Next**.
d) In the **Select Role Services** window, check these check boxes and click **Next**.

   - Certificate Authority
   - Certificate Authority Web Enrollment
   - Online Responder

e) In the **Specify Setup Type** window, click **Standalone**.
f) In the **Specify CA Type** window, click **Root CA**.
g) In the **Set Up Private Key** window, click **Create a new private key**.
h) In the **Configure Cryptography for CA** window, choose the default cryptographic service provider.
i) In the **Configure CA Name** window, enter a common name to identify the CA.
j) In the **Set Validity Period** window, set the validity period for the certificate generated for the CA.

   Note The CA issues valid certificates only up to the expiration date that you specify.

k) In the **Configure Certificate Database** window, choose the default certificate database locations.
l) In the **Confirm Installation Selections** window, click **Install**.
m) In the **Installation Results** window, verify that the **Installation Succeeded** message displays for all components and click **Close**.

   Note The Active Directory Certificate Services is now listed as one of the roles on the Server Manager.

What to do next

Generating a CSR – Running Windows Server 2008 , on page 55

Generation of a CSR on IIS of a Microsoft Exchange Server

Generating a CSR – Running Windows Server 2003

You must generate a Certificate Signing Request (CSR) on the IIS Server for Exchange, which is subsequently signed by the CA Server. If the Certificate has the Subject Alternative Name (SAN) field populated, it must match the Common Name (CN) of the certificate.

Before you begin

[Self-signed Certificates] Install the certificate CA service if required.

Procedure

Step 1 From Administrative Tools, open **Internet Information Services**.

a) Right-click **Default Web Site**.
b) Choose **Properties**.

Step 2 Choose the **Directory Security** tab.

Step 3 Choose **Server Certificate**.

Step 4 Click **Next** when the **Web Server Certificate** wizard displays.

Step 5 Complete the **Server Certificate** wizard:

a) In the **Server Certificate** window, choose **Create a new certificate** and click **Next**.
b) In the **Delayed or Immediate Request** window, choose **Prepare the request now, but send it later** and click **Next**.
c) In the **Name and Security Settings** window, accept the Default Web Site certificate name, choose **1024** for the bit length, and click **Next**.
d) In the **Organization Information** window, enter your Company name in the Organization field, the organizational unit of your company in the Organizational Unit field, and click **Next**
e) In the **Your Site's Common Name** window, enter the Exchange Server hostname or IP address and click **Next**.

Note The IIS certificate Common Name that you enter is used to configure the Presence Gateway on the IM and Presence Service, and must be identical to the Host (URI or IP address) you are trying to reach.

f) In the **Geographical Information** window, enter your geographical information, as follows, and click **Next**.

- Country/region
- State/province
- City/locality

g) In the **Certificate Request File Name** window, enter an appropriate filename for the certificate request, specify the path and file name where you want to save your CSR, and click **Next**.

Note Make sure that you save the CSR without any extension (.txt) and remember where you save it because you need to be able to find this CSR file after. Only use Notepad to open the file.

h) In the **Request File Summary** window, confirm that the information is correct in the **Request File Summary** window and click **Next**.
i) In the **Web Server Certificate Completion** window, click **Finish**.

What to do next

Submitting a CSR to the CA Server/Certificate Authority, on page 56

Generating a CSR – Running Windows Server 2008

You must generate a Certificate Signing Request (CSR) on the IIS Server for Exchange, which is subsequently signed by the CA Server.

Procedure

Step 1 From Administrative Tools, open the **Internet Information Services (IIS) Manager** window.

Step 2 Under Connections in the left pane of the IIS Manager, choose the Exchange Server.

Step 3 Double-click **Server Certificates**.

Step 4 Under Actions in the right pane of the IIS Manager, choose **Create Certificate Request**.

Step 5 Complete the **Request Certificate** wizard:

a) In the **Distinguished Name Properties** window, enter the following information:

- In the **Common Name** field, enter the Exchange Server hostname or IP address.
- In the **Organization** field, enter your company name
- In the **Organizational Unit** field, enter the organizational unit that your company belongs to.

b) Enter your geographic information as follows and click **Next**.

- City/locality
- State/province
- Country/region

Note The IIS certificate Common Name that you enter is used to configure the Presence Gateway on the IM and Presence Service, and must be identical to the host (URI or IP address) you are trying to reach.

c) In the **Cryptographic Service Provider Properties** window, accept the default Cryptographic service provider, choose **2048** for the bit length, and click **Next**.
d) In the **Certificate Request File Name** window, enter the appropriate filename for the certificate request and click **Next**.

Note Make sure that you save the CSR without any extension (.txt) and remember where you save it because you need to be able to find this CSR file later. Only use Notepad to open the file.

e) In the **Request File Summary** window, confirm that the information is correct and click **Next**.
f) In the **Request Certificate Completion** window, click **Finish**.

What to do next

Submitting a CSR to the CA Server/Certificate Authority, on page 56

Submitting a CSR to the CA Server/Certificate Authority

We recommend that the default SSL certificate, generated for Exchange on IIS, should use the Fully Qualified Domain Name (FQDN) of the Exchange Server and be signed by a Certificate Authority that the IM and Presence Service trusts. This procedure allows the CA to sign the CSR from Exchange IIS. Perform the following procedure on your CA Server, and configure the FQDN of the Exchange Server in the:

- Exchange certificate.
- Presence Gateway field of the Exchange Presence Gateway in **Cisco Unified CM IM and Presence Administration**.

Before you begin

Generate a CSR on IIS of the Exchange Server.

Procedure

Step 1 Copy the certificate request file to your CA Server.

Step 2 Open one of the following URLs:

- Windows 2003 or Windows 2008: http://*locall_server*/certserv

or

- Windows 2003: http://127.0.0.1/certserv
- Windows 2008: http://127.0.0.1/certsrv

Step 3 Choose **Request a certificate**.

Step 4 Choose **advanced certificate request**.

Step 5 Choose **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

Step 6 Using a text editor like Notepad, open the CSR that you generated.

Step 7 Copy all information from and including

-----BEGIN CERTIFICATE REQUEST

to and including

END CERTIFICATE REQUEST-----

Step 8 Paste the content of the CSR into the Certificate Request text box.

Step 9 (Optional) By default the Certificate Template drop-down list defaults to the Administrator template, which may or may not produce a valid signed certificate appropriate for server authentication. If you have an enterprise root CA, choose the Web Server certificate template from the Certificate Template drop-down list. The Web Server certificate template may not display, and therefore this step may not apply, if you have already modified your CA configuration.

Step 10 Click **Submit**.

Step 11 In the **Administrative Tools** window, choose **Start** > **Administrative Tools** > **Certification** > **Authority** > **CA name** > **Pending Request** to open the **Certification Authority** window. The **Certificate Authority** window displays the request you just submitted under Pending Requests.

Step 12 Right click on your request, and complete these actions:

- Navigate to **All Tasks**.
- Choose **Issue**.

Step 13 Choose **Issued certificates** and verify that your certificate has been issued.

What to do next

Downloading a Signed Certificate, on page 57

Downloading a Signed Certificate

Before you begin

[Self-signed Certificates] Submit the Certificate signing request (CSR) to the CA server.

[Third-Party Certificates] Request the CSR from your Certificate Authority.

Procedure

Step 1 In Administrative Tools, open the Certification Authority. The Certificate Request that you issued displays in the Issued Requests area.

Step 2 Right click the request and choose **Open**.

Step 3 Choose the **Details** tab.

Step 4 Choose **Copy to File**.

Step 5 When the **Certificate Export** wizard displays, click **Next**.

Step 6 Complete the **Certificate Export** wizard:

a) In the **Export File Format** window, choose **Base-64 encoded X.509** and click **Next**.

b) In the **File to Export** window, enter the location where you want to store the certificate, use cert.cer for the certificate name, and choose `c:\cert.cer`.

c) In the **Certificate Export Wizard Completion** window, review the summary information, verify that the export was successful, then click **Finish**.

Step 7 Copy or FTP the cert.cer to the computer that you use to administer the IM and Presence Service.

What to do next

Upload of Signed Certificate onto Exchange IIS, on page 84

Upload a signed certificate for your server type:

- Uploading a Signed Certificate – Running Windows 2003, on page 58

- Uploading a Signed Certificate – Running Windows 2008, on page 59

Upload of Signed Certificate onto Exchange IIS

Uploading a Signed Certificate – Running Windows 2003

This procedure takes the signed CSR and uploads it onto IIS. To upload the signed certificate, perform the following steps on the computer that you use to administer the IM and Presence Service.

Before you begin

[Self-signed Certificates] Download the signed certificate.

[Third-party Certificates] Your Certificate Authority provides you with the signed certificate.

Procedure

Step 1 From Administrative Tools, open **Internet Information Services**.

Step 2 Complete the following steps in the **Internet Information Services** window:

a) Right-click **Default Web Site**.

b) Choose **Properties**.

Step 3 In the **Default Web Site Properties** window, complete the following steps:

a) Choose the **Directory Security** tab.

b) Choose **Server Certificate**.

Step 4 When the **Web Server Certificate** wizard window displays, click **Next** .

Step 5 Complete the **Web Server Certificate** wizard:

a) In the **Pending Certificate Request** window, choose **Process the pending request and install the certificate** and click **Next**.

b) In the **Process a Pending Request** window, click **Browse** to locate your certificate and navigate to the correct path and filename.

c) In the **SSL Port** window, enter 443 for the SSL port and click **Next**.

d) In the **Web Server Certificate Completion** window, click **Finish**.

Tip

If your certificate is not in the trusted certificates store, the signed CSR is not trusted. To establish trust, complete these actions:

- Under the **Directory Security** tab, click **View Certificate**.
- Choose **Details** > **Highlight root certificate**, and click **View**.
- Choose the **Details** tab for the root certificate and install the certificate.

What to do next

Downloading a Root Certificate, on page 59

Uploading a Signed Certificate – Running Windows 2008

This procedure takes the signed CSR and uploads it onto IIS. To upload the signed certificate, perform the following step on the computer that you use to administer the IM and Presence Service.

Before you begin

[Self-signed Certificates] Download the signed certificate.

[Third-party Certificates] Your Certificate Authority provides the signed certificate.

Procedure

Step 1 From Administrative Tools, open the **Internet Information Services (IIS) Manager** window.

Step 2 Under Connections in the left pane of the IIS Manager, choose the Exchange Server.

Step 3 Double-click **Server Certificates**.

Step 4 Under Actions in the right pane of the IIS Manager, choose **Complete Certificate Request**.

Step 5 In the **Specify Certificate Authority Response** window, complete these actions:

a) To locate your certificate, choose the ellipsis [...].
b) Navigate to the correct path and filename.
c) Enter a user-friendly name for your certificate.
d) Click **Ok**. The certificate that you completed displays in the certificate list.

Step 6 In the **Internet Information Services** window, complete the following steps to bind the certificate:

a) Choose **Default Web Site**.
b) Under Actions in the right pane of the IIS Manager, choose **Bindings**.

Step 7 Complete the following steps in the **Site Bindings** window:

a) Choose **https**.
b) Choose **Edit**.

Step 8 In the **Edit Site Binding** window, complete the following steps :

a) Choose the certificate that you just created from the SSL certificate drop-down list. The name that you applied to the certificate displays.
b) Click **Ok**.

What to do next

Downloading a Root Certificate, on page 59

Downloading a Root Certificate

Before you begin

Upload the Signed Certificate onto Exchange IIS.

Procedure

Step 1 Log in to your CA Server user interface and open a web browser.

Step 2 Open the URL specific to your Windows platform type:

a) Windows Server 2003 – http://127.0.0.1/certserv

b) Windows Server 2008 – https://127.0.0.1/certsrv

Step 3 Choose **Download a CA certificate, certificate chain, or CRL**.

Step 4 For the Encoding Method, choose **Base 64**.

Step 5 Click **Download CA Certificate**.

Step 6 Save the certificate, **certnew.cer**, to the local disk.

Tip

If you do not know the Subject Common Name (CN) of the root certificate, you can use an external certificate management tool to find this information. On a Windows operating system, right-click the certificate file with a .cer extension and open the certificate properties.

What to do next

Upload a Root Certificate to the IM and Presence Service Node, on page 60

Upload a Root Certificate to the IM and Presence Service Node

Before you begin

- [Self-signed Certificates] Download the root certificate.
- [Third-party Certificates] Request the root certificate from your Certificate Authority. If you have a third-party CA-signed Exchange server certificate, note that you must upload all CA certificates in the certificate chain to the IM and Presence Service as a CiscoUnified Presence Trust certificate (cup-trust).

Procedure

Step 1 Use the Certificate Import Tool in **Cisco Unified CM IM and Presence Administration** to upload the certificate:

Upload the certificate via:	Actions
Certificate Import Tool in **Cisco Unified CM IM and Presence Administration**. The Certificate Import tool simplifies the process of installing trust certificates on the IM and Presence Service and is the primary method for certificate exchange. The tool allows you to specify the host and port of the Exchange server and attempts to download the certificate chain from the server. Once approved, the tool automatically installs missing certificates. **Note** This procedure describes one way to access and configure the Certificate Import Tool in **Cisco Unified CM IM and Presence Administration**. You can also view a customized version of the Certificate Import Tool in **Cisco Unified Presence Administration** when you configure the Exchange Presence Gateway for a specific type of calendaring integration (Log in to **Cisco Unified CM IM and Presence Administration** and choose **Presence** > **Gateways**).	**a.** Log in to the **Cisco Unified CM IM and Presence Admi** **b.** Choose **System** > **Security** > **Certificate Import Tool**. **c.** Choose **IM and Presence(IM/P) Trust** as the Certificate to install the certificates. This stores the Presence Engine t Exchange integration. **d.** Enter one of these values to connect with the Exchange Se • IP address • Hostname • FQDN The value that you enter in this Peer Server field must exa hostname or FQDN of the Exchange Server. **e.** Enter the port that is used to communicate with the Excha match the available port on the Exchange Server. **f.** Click **Submit**. After the tool finishes, it reports these state • Peer Server Reachability Status — indicates whether Service can reach (ping) the Exchange Server. See Trou Connection Status, on page 93. • SSL Connection/Certificate Verification Status — inc Certificate Import Tool succeeded in downloading ce peer server and whether or not a secure connection ha the IM and Presence Service and the remote server. S Connection Certificate Status , on page 94.

Step 2 If the Certificate Import Tool indicates that certificates are missing (typically the CA certificate is missing on Microsoft servers), manually upload the CA certificate(s) using the **Cisco Unified OS Admin Certificate Management** window.

Upload the certificate via:	Actions
Cisco Unified IM and Presence Operating System Administration If the Exchange Server does not provide the CA certificates during the SSL/TLS handshake, you cannot use the Certificate Import Tool to import those certificates. In this case, you must manually import the missing certificates using the Certificate Management tool in (Log in to **Cisco Unified IM and Presence Operating System Administration**. Choose **Security** > **Certificate Management**).	**a.** Copy or FTP the **certnew.cer** certificate file to the computer th your IM and Presence Service node. **b.** Log in to the **Cisco Unified IM and Presence Operating Sy** user interface. **c.** Choose **Security** > **Certificate Management**. **d.** In the **Certificate List** window, choose **Upload Certificate/C** **e.** Complete these actions when the **Upload Certificate/Certific** opens: • From the Certificate Name drop-down list, choose **cup-t** • Enter the root certificate name without any extension. **f.** Click **Browse** and choose **certnew.cer**. **g.** Click **Upload File**.

Step 3 Return to the Certificate Import Tool (Step 1, on page 86) and verify that all status tests succeed.

Step 4 Restart the CiscoPresence Engine and SIP Proxy service after you upload all Exchange trust certificates. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Feature Services**.

Tips

The IM and Presence Service allows you to upload Exchange Server trust certificates with or without a Subject Common Name (CN).

What to do next

Configure the IM and Presence Service, on page 67

Enabling Calendar Integration

Calendar integration is enabled by the administrator, either on an individual basis or for groups of users.

Note Ensure the Presence Gateway is configured on Cisco Unified Communications Manager. For more information, see Configure a Presence Gateway for Microsoft Exchange Integration , on page 75.

Enabling Calendar Integration for Individual Users

Use this procedure to configure Microsoft Outlook calendar integration for an individual end user.

Procedure

Step 1 Log in to the **Cisco Unified CM Administration** user interface.

Step 2 Choose **User Management** > **End User**.

Step 3 Click **Find** and select an end user.

Step 4 Check the **Enable User for Unified CM IM and Presence** check box.

Step 5 Check the **Include meeting information in presence** check box.

Step 6 Click **Save**.

Enabling Calendar Integrations in Bulk

Procedure

Step 1 On a Cisco Unified Communications Manager node, log in to the **Cisco Unified CM Administration** user interface.

Step 2 Enabling calendar integrations in bulk can be performed from the following windows:

a) **Bulk Administration** > **Users** > **Insert Users**.

b) **Bulk Administration** > **Users** > **Update Users** > **Query**.

c) **Bulk Administration** > **Users** > **Update Users** > **Custom File**.

Note For information on the different types of update options, refer to the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Step 3 For all end users for whom you want to enable calendar integration, make sure that the following end user configuration options are checked:

- **Enable User for Unified CM IM and Presence**
- **Include meeting information in Presence**

Step 4 If you are updating from a csv file, in the appropriate Users area, choose a File Name.

Note Click **View Sample File** for the correct file format.

Step 5 Click **Run Immediately** or **Run Later**.

Step 6 Click **Submit**.

[Optional] Configure the Frequency of Exchange Calendar Notifications Sent Over Exchange Web Services

Note This procedure only applies if you are integrating Microsoft Exchange Server 2007, 2010, or 2013 over Exchange Web Services (EWS).

The EWS Status Frequency parameter specifies an interval (in minutes) that determines how long it takes before the Exchange Server updates the subscription on the IM and Presence Service. By default this parameter is 60 minutes. Shorten this duration if you want the Presence Engine on the IM and Presence Service to detect that it has lost the subscription more frequently than every 60 minutes (default). Error detection improves if you shorten the duration but there is a corresponding increased load on the Exchange Server and the IM and Presence Service node.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface.

Step 2 Choose **System** > **Service Parameters**.

Step 3 From the Server drop-down list, choose the IM and Presence Service node.

Step 4 From the Service drop-down list, choose Cisco Presence Engine (Active).

Step 5 In the Calendaring Configuration (Parameters that apply to all servers) area, edit the parameter value in the EWS Status Frequency field, this parameter limit is 1440 minutes. By default this parameter is 60 minutes.

Step 6 Click **Save**.

What to do next

EWS Status Frequency parameter changes are updated incrementally as calendar integration occurs on a per-user basis. However, we recommend that you restart the Cisco Presence Engine to effect the parameter change for all users at once. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Service Activation**.

[Optional] Configure the Microsoft Exchange Notification Port

This topic only applies if you want the Cisco Presence Engine to listen for incoming notifications from the Exchange Server on another port specific to your network configuration.

With an EWS integration, a TCP port is used by default to receive the HTTP notifications.

Before you begin

If you change from the default port, make sure that the replacement port that you assign is not already in use.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface.

Step 2 Choose **System** > **Service Parameters**.

Step 3 From the Server drop-down list, choose the IM and Presence Service node.

Step 4 From the Service drop-down list, choose Cisco Presence Engine (Active).

Step 5 In the Calendaring Configuration area, edit the parameter value for the Microsoft Exchange Notification Port field and click **Save**.

What to do next

We recommend that you restart the Cisco Presence Engine to effect the parameter change for all users at once. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Control Center - Feature Services**.

Tip

- If you change from the default port, the Cisco Presence Engine continues to use the existing calendar information for users, (including the number of meetings and the start and end times) until such time as the Exchange subscription for the user is renewed. It may take up to an hour for the Cisco Presence Engine to receive notifications that a user’s calendar has changed.
- We recommend that you restart the Cisco Presence Engine to effect the change for all users at once.

[Optional] Configuring the Duration Range of Microsoft Exchange Calendar Notifications

By default, the Cisco Presence Engine allows for meeting/busy notifications to be sent 50 seconds after the top-of-the-minute. If you have a small user base, we recommend that your shorten this delay using the formula specified in this procedure. However, note that this topic is optional and only applies if you want to change the duration range for any reason specific to your network configuration.

Before you begin

Use this formula to configure this field value (in seconds): Maximum number of assigned users / 100. For example, if a node has a maximum number of users of 1000, then the offset range is 10 seconds.

Procedure

Step 1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface.

Step 2 Choose **System** > **Service Parameters**.

Step 3 From the Server drop-down list, choose the IM and Presence Service node.

Step 4 From the Service drop-down list, choose Cisco Presence Engine (Active).

Step 5 In the Calendaring Configuration area, edit the parameter value in the Calendar Spread field. This parameter limit is 59 seconds. If meetings start or end more than one minute late, it interferes with meeting start/end counters and notifications. By default this parameter is 50.

Step 6 Click **Save**.

What to do next

Calendar Spread parameter changes are updated incrementally as calendar integration occurs on a per-user basis. However, we recommend that you restart the Cisco Presence Engine to effect the parameter change for all users at once. Log in to **Cisco Unified IM and Presence Serviceability**. Choose **Tools** > **Control Center - Feature Services**.

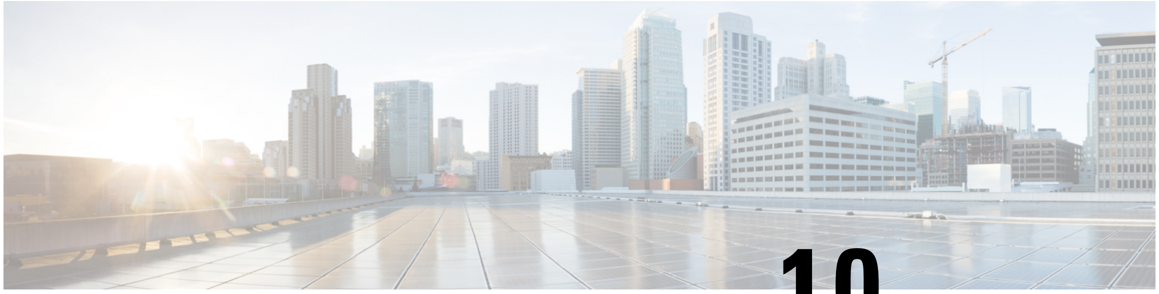
Tip If a very large number of users transition either in or out of meetings, a mass notification event occurs that may delay some notifications up to a few minutes.

Other Microsoft Exchange Calendaring Parameters

There are three other Exchange calendaring parameters that you can configure in the **Service Parameters** window of **Cisco Unified CM IM and Presence Administration**:

- Exchange Timeout (seconds) — the duration, in seconds, before a request made to an Exchange Server times out.
- Exchange Queue — the length of the request queue.
- Exchange Threads — the number of threads used to service Exchange requests.

Caution We do not recommend that you change the default settings of these parameters because any changes may adversely affect your Exchange integration. Contact Cisco Technical Assistance Center (TAC) for support.



CHAPTER 10

Troubleshooting Exchange Calendaring Integrations

Troubleshooting Exchange Server Connection Status

Exchange Server connection status displays under the **Cisco Unified CM IM and Presence Administration** window after you configure the Exchange Presence Gateway for an Exchange Web Services (EWS) calendaring integration (choose **Presence** > **Gateways**). The Exchange Server Status area in the **Presence Gateway Configuration** window reports the status on the connection between the IM and Presence Service and the Exchange Server.

Note You can add, update or delete one or more EWS servers with no maximum limit. However, the Exchange Server Status area in the **Presence Gateway Configuration** window is designed to only verify and report status of the first 10 EWS servers that you configure.

.

Test	Status Description and Recommended Action
Exchange Reachability (pingable)	The IM and Presence Service successfully reached (pinged) the Excha
Exchange Reachability (unreachable)	The IM and Presence Service failed to ping the Exchange Server. The incorrect field value or an issue with the customer's network, for exam To resolve this, ensure that the Presence Gateway field contains the corr the Exchange Server over the network. Note that the UI does not requi be the Subject CN value. If you have connection problems with the Exchange Server, also see the **CM IM and Presence Administration** and implement the recommen **System Troubleshooter**.

Troubleshooting SSL Connection Certificate Status

SSL Connection/Certificate Verification status displays in **Cisco Unified CM IM and Presence Administration** window when you configure the Exchange Presence Gateway for an Exchange Web Services (EWS) calendaring integration (choose **Presence** > **Gateways**). The Exchange Server Status area in the **Presence Gateway Configuration** window indicates if there is a certificate Subject CN mismatch or a SAN mismatch.

Note You can add, update or delete *one or more* EWS servers with no maximum limit. However, the Troubleshooter on the **Presence Gateway** window is designed to only verify and report status of the first 10 EWS servers that you configure.

Test	Status Description and Recommended Action
SSL Connection/Certificate Verification - Verified	The IM and Presence Service verified the SSL connection with the Exchang

Test	Status Description and Recommended Action
SSL Connection/Certificate Verification Failed - Certificate Missing From Chain **Note** These instructions describe the view of the customized Certificate Import Tool. If you are simply verifying connection status, the tool indicates the verified status but you do not have the option to **Save**.	One or more certificates that the IM and Presence Service requires to est are missing. The Certificate Viewer can provide details of the missing c Complete these steps in the Certificate Viewer to display any missing ce **1.** Chose **Configure** to open the Certificate Viewer. **2.** Check the **Accept Certificate Chain** check box . **3.** Click **Save**. **4.** The certificate chain details display. Note any certificates with a stat **5.** Close the Certificate Viewer. To complete the certificate chain, you must: **1.** Download the missing certificates files from the Exchange Server. **2.** Copy or FTP the missing certificate files to the computer that you us **3.** Use **Cisco Unified IM and Presence OS Administration** to uploa **Troubleshooting Tips** • If the certificates are not available in the Certificate Viewer, you ma certificates from the Exchange Server, and upload these certificates in as follows: • Log in to the **Cisco Unified IM and Presence OS Administr** complete the certificate chain. • Return to the **Presence Gateway Configuration** window und **Administration** user interface, reopen the Certificate Viewer, now have a status of Verified. • You must restart the Cisco Presence Engine after you upload Excha • Log in to **Cisco Unified IM and Presence Serviceability** user inte • Choose **Tools** > **Service Activation**. Note that this can affect Calen • Choose either **Configure** or **View** to launch the Certificate Chain V issues with the certificate chain that the IM and Presence Service c the missing certificates scenario described above. Once you success Connection / Certificate Verification status updates to Verified and

Test	Status Description and Recommended Action
SSL Connection/Certificate Verification Failed- Subject CN Mismatch	The Presence Gateway field value must match the Subject CN value of the resolve this by entering the correct value in the Presence Gateway field. Verify that your entry in the Presence Gateway field is correct as follows: **1.** Re-enter the correct Subject CN value in the Presence Gateway field. T Gateway field value to ping the server. The host (FQDN or IP address) th Subject Common Name. **2.** Click **Save**. **Tip** Choose either **Configure** or **View** to launch the Certificate Chai are any issues with the certificate chain downloaded from the E certificates scenario described above. Once you successfully in Connection / Certificate Verification status updates to Verified
SSL Connection/Certificate Verification Failed - SAN Mismatch	The Presence Gateway field value must match one of the Subject Alternativ Certificate Chain. You can resolve this by entering the correct value in the F Verify that your entry in the Presence Gateway field is correct as follows: **1.** Re-enter the correct SAN value in the Presence Gateway field. The IM field value to ping the server. The host (FQDN or IP address) that you e certificate Subject Alternative Name. **2.** Click **Save**. **Tip** Choose either **Configure** or **View** to launch the Certificate Chai are any issues with the certificate chain downloaded from the E certificates scenario described above. Once you successfully in Connection / Certificate Verification status updates to Verified
SSL Connection/Certificate Verification Failed - Bad Certificates	Information in the certificate is incorrect, which renders it invalid. Typically, this occurs if the certificate matches the required Subject CN but Exchange Server regenerates the certificate but the IM and Presence Servic To resolve this, complete these actions: • Choose the logs to determine the cause of the error. • If the error is due to a bad signature, you need to remove the outdated CiscoUnified IM and Presence OS Administration, and then upload a n OS Administration. • If the error is due to an unsupported algorithm, you need to upload a ne in CiscoUnified IM and Presence OS Administration.
SSL Connection / Certificate Verification Failed - Network Error	Due to network issues, for example, a no-response timeout, the IM and Pres We recommend that you verify the network connectivity to the Exchange S accepting connections using the correct IP address and port number.
SSL Connection/Certificate Verification Failed	Verification failed for a non-specific reason or because the IM and Presence We recommend that you review the debug log files for more information.

Issues Known to Impact Microsoft Exchange Integrations

This section describes known issues that are common or specific to Microsoft Exchange Server 2007, 2010, and 2013.

Scale Limitations for Calendar Integrations

Cisco Unified Communications Manager IM and Presence Service and Exchange calendaring integrations have been validated with up to X% of the users subscribing to calendar presence and with up to Y% of the users doing simultaneous calendar transitions (for example, joining or leaving meetings simultaneously). See the table below for percentage values pertaining to specific releases of Cisco Unified Presence.

Table 18: Scale Limitations for Specific Cisco Unified Presence Releases

Software Release	% of Users Subscribing to Calendar Presence	% of Users Performing Simultaneous Caler Transitions
8.5(1)	50	30
8.5(2) and later	100	50

Calendar State Does Not Update if a User Moves Between Microsoft Exchange Servers

Problem

If an Exchange administrator moves a user from one Exchange Server to another in an Exchange integration, the calendaring state change does not update for that user.

Cause

The condition occurs because the Exchange Server does not signal when a user is moved from one server to another.

Solution

The IM and Presence Service administrator or user must disable and then reenable calendar integration for that user *after* the Exchange administrator has moved the user from one Exchange Server to another.

LDAP User Removal Takes at Least 24 Hours to Replicate on the IM and Presence Service

Problem

If a user is deleted from LDAP, the user state changes to Inactive on CiscoUnified Communications Manager and user authentication on client applications subsequently fails. However, it has been observed during testing that once CiscoUnified Communications Manager synchronizes the change from LDAP, the user is not removed for 24 hours *after* the synchronization occurred (either by the Administrator forcing the synchronization or scheduling it to occur at a specific time).

The Cisco Sync Agent on the IM and Presence Service does not synchronize any user state change until the user is removed. Until then, that user still exists on CiscoUnified Communications Manager and all IM and Presence Service capabilities (including Exchange calendaring subscriptions) remain licensed for that user for 24 hours. This delay means that users who were logged in to Cisco Jabber before the user was removed from LDAP are not logged out automatically. The user's pre-existing calendar state (Available, Busy) persists for that user on the IM and Presence Service until the user logs out of the client.

Cause

The condition occurs when CiscoUnified Communications Manager is set up and LDAP authentication is used. When a user is deleted from LDAP, calendaring subscriptions continue to be established and updated for that user on the IM and Presence Service for a period of at least 24 hours.

Solution

If a user is removed from LDAP, you can manually remove the license for that user so that the IM and Presence Service ends the Exchange calendaring subscriptions with immediate effect and logs the user out of the client application. Otherwise, be aware that there may be a 24 hour delay.

Verifying That the Microsoft Exchange Server URL Contains the Localized Word for Calendar

If you are localizing your Calendaring integration, verify that the Exchange Server URL contains the localized word for Calendar.

Procedure

Step 1 Install the same language locales (load the locale installer) on both the IM and Presence Service and Cisco Unified Communications Manager. For more information about installing locales on the IM and Presence Service, see Configuration of Multilingual Support for Calendar Integration.

Step 2 Restart the IM and Presence Service node, and log in to the **Cisco Unified CM IM and Presence Administration** user interface.

Step 3 Find and delete the existing Exchange Presence Gateway that supports a different locale for calendaring (choose **Presence** > **Gateways**).

Step 4 Add a new Exchange Presence (Outlook) Gateway. Click **Add New**.

Step 5 Verify in the database (pebackendgateway table) that the 'localecalendarname' attribute is in whichever language locale you have installed.

Step 6 Ensure the user locale is set after the locale is installed on both the IM and Presence Service and toggling the user locale on the Cisco Unified Communications Manager, if necessary.