Microsoft Exchange for IM and Presence Service on Cisco Unified Communications Manager, Release 11.5(1)

First Published: June 08, 2016

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

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Preface** 1

Introduction 1

Audience 1

Organization 1

Conventions 2

Obtaining Documentation and Submitting a Service Request 3

CHAPTER 2 **Introduction to IM and Presence Service Integration with Microsoft Exchange** 5

Overview 5

Deployment 6

Exchange Web Services 6

Microsoft Outlook Calendaring States on the IM and Presence Service 6

Presence Gateway Options 7

Restrictions and Limitations 7

CHAPTER 3 **Planning for IM and Presence Service Integration with Microsoft Exchange** 9

Prerequisite Configuration Tasks 9

Configuration Considerations 10

Integration with Microsoft Exchange Server over Exchange Web Services 10

Administrative Roles and Permissions in Exchange Server 10

Presence Gateway Configuration for Exchange Server Integrations 11

Known Issues with Exchange Web Services Integration 12

Security Considerations 12

Windows Security Policy Settings 12

Getting More Information 12

CHAPTER 4 **Integrate Microsoft Exchange with the IM and Presence Service over Exchange Web Services** 13

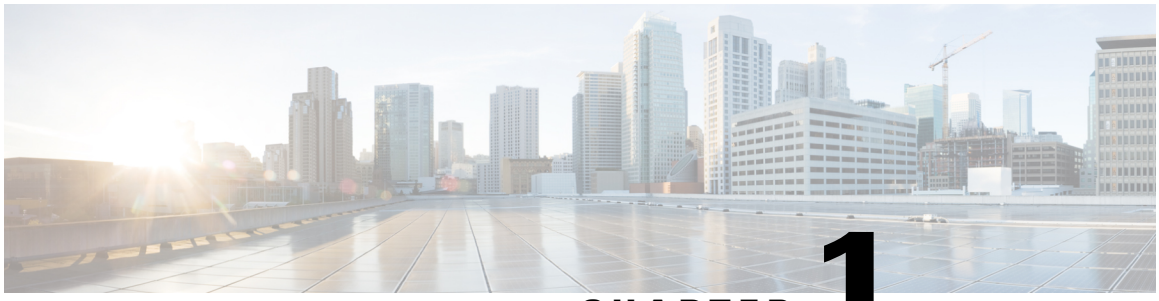
Microsoft Exchange 2007 Configuration over Exchange Web Services 13

Windows Security Policy Settings 14
Verifying Windows Security Settings 14
Grant Users Permission to Sign in to the Service Account Locally 14
Configuring Microsoft Exchange 2007 on Windows Server 2003 15
Configuring Microsoft Exchange 2007 on Windows Server 2008 15
Setting Impersonation Permissions at the Server Level 16
Setting Active Directory Service Extended Permissions for the Service Account 17
Granting Send As Permissions to the Service Account and User Mailboxes 17
Granting Impersonation Permissions to the Service Account and User Mailboxes 18
Verifying Permissions on the Microsoft Exchange 2007 Account 19
Microsoft Exchange 2010 and 2013 Configuration over Exchange Web Services 19
Windows Security Policy Settings 21
Verifying Windows Security Settings 21
Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2010 21
Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2013 23
Verify Permissions on the Microsoft Exchange 2010 Accounts 24
Verify Permissions on the Microsoft Exchange 2013 Accounts 25
Enable Authentication on the Exchange Virtual Directories 26
Enabling Authentication on Exchange 2007 Running Windows Server 2003 27
Enable Authentication on Exchange 2010 and 2013 Running Windows Server 2008 27

CHAPTER 5 **Configure the IM and Presence Service to Integrate with the Microsoft Exchange Server** 29
Configure a Presence Gateway for Microsoft Exchange Integration 29
Configure Exchange 2007, 2010, or 2013 as a Presence Gateway over Exchange Web Services 30
SAN and Wildcard Certificate Support 31
Configure Secure Certificate Exchange Between the IM and Presence Service and Microsoft Exchange 32
How to Install the Certificate Authority Service 32
Installing a CA on Windows Server 2003 32
Installing a CA on Windows Server 2008 33
Generation of a CSR on IIS of a Microsoft Exchange Server 34
Generating a CSR – Running Windows Server 2003 34

Generating a CSR – Running Windows Server 2008 35
Submitting a CSR to the CA Server/Certificate Authority 36
Downloading a Signed Certificate 37
Upload of Signed Certificate onto Exchange IIS 38
Uploading a Signed Certificate – Running Windows 2003 38
Uploading a Signed Certificate – Running Windows 2008 39
Downloading a Root Certificate 39
Upload a Root Certificate to the IM and Presence Service Node 40
Enabling Calendar Integration 42
Enabling Calendar Integration for Individual Users 43
Enabling Calendar Integrations in Bulk 43
[Optional] Configure the Frequency of Exchange Calendar Notifications Sent Over Exchange Web Services 43
[Optional] Configure the Microsoft Exchange Notification Port 44
[Optional] Configuring the Duration Range of Microsoft Exchange Calendar Notifications 45
Other Microsoft Exchange Calendaring Parameters 46

CHAPTER 6 **Troubleshooting Exchange Calendaring Integrations** 47
Troubleshooting Exchange Server Connection Status 47
Troubleshooting SSL Connection Certificate Status 48
Issues Known to Impact Microsoft Exchange Integrations 52
Scale Limitations for Calendar Integrations 52
Calendar State Does Not Update if a User Moves Between Microsoft Exchange Servers 53
LDAP User Removal Takes at Least 24 Hours to Replicate on the IM and Presence Service 53
Verifying That the Microsoft Exchange Server URL Contains the Localized Word for Calendar 54



CHAPTER 1

Preface

- Introduction, page 1
- Audience, page 1
- Organization, page 1
- Conventions, page 2
- Obtaining Documentation and Submitting a Service Request, page 3

Introduction

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

Audience

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

Organization

This guide contains the following sections:

Chapter	Title	Description
1	Introduction to IM and Presence Service Integration with Microsoft Exchange, on page 5	Introduction to Microsoft Exchange Integration with the IM and Presence Service.
2	Planning for IM and Presence Service Integration with Microsoft Exchange, on page 9	Describes the prerequisite configuration tasks, configuration and security considerations, and how to get more information.

Chapter	Title	Description
3	Microsoft Exchange 2007 Configuration over Exchange Web Services, on page 13	Describes the integration of the IM and Presence Service with Microsoft Exchange Server 2007, 2010, and 2013 over Exchange Web Services.
4	Configure the IM and Presence Service to Integrate with the Microsoft Exchange Server, on page 29	Describes common configuration tasks.
5	Troubleshooting Exchange Calendaring Integrations, on page 47	Describes the most common 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.

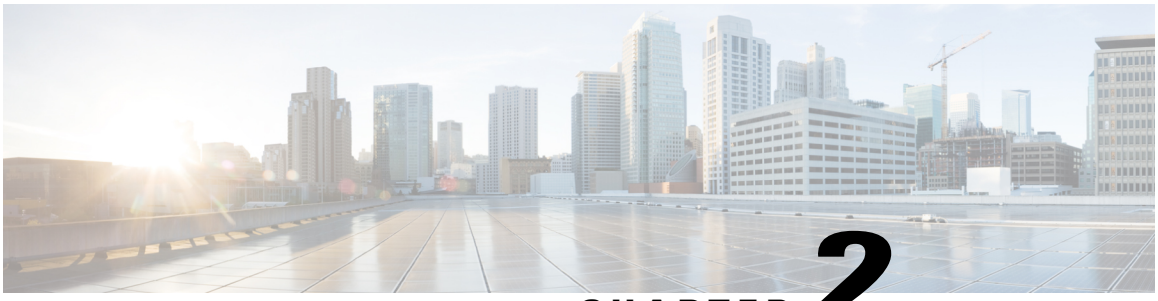
Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

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

Introduction to IM and Presence Service Integration with Microsoft Exchange

- Overview, page 5
- Deployment, page 6
- Microsoft Outlook Calendaring States on the IM and Presence Service, page 6
- Restrictions and Limitations , page 7

Overview

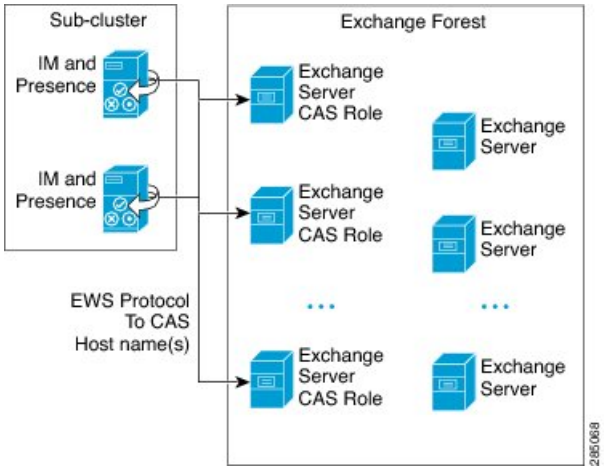
Microsoft Exchange integration with the IM and Presence Service allows users to incorporate their calendar/meeting status in Microsoft Outlook into their availability status on the IM and Presence Service.

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 Exchange 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. 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 1: 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.

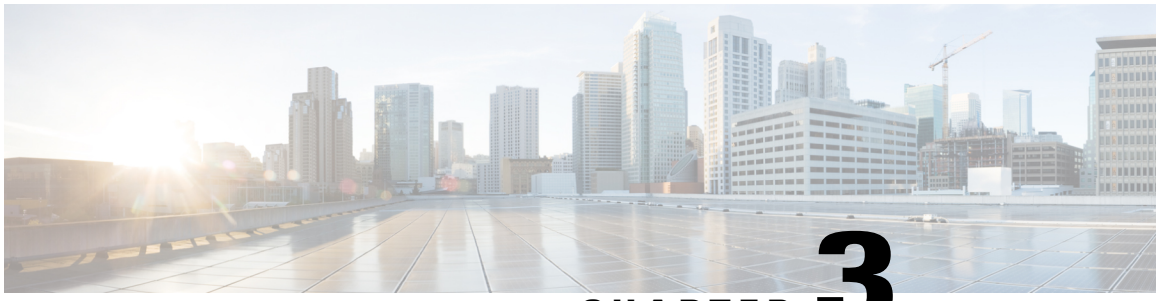
Presence Gateway Options

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

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.



CHAPTER 3

Planning for IM and Presence Service Integration with Microsoft Exchange

- Prerequisite Configuration Tasks , page 9
- Configuration Considerations, page 10
- Security Considerations, page 12
- Getting More Information , page 12

Prerequisite Configuration Tasks

Before you configure Microsoft Exchange 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 2: Compatibility Matrix

Component	Install Compatible Version
Windows Server	• Service Packs for Windows Server 2003 (SP2) • Service Packs for Windows Server 2008 (SP2) • Service Packs for Windows Server 2012 (Standard)
Cisco Unified Communications Manager	The Cisco Unified Communications Manager release must match the IM and Presence Service release.
IM and Presence Service	The IM and Presence Service release must match the Cisco Unified Communications Manager release.
Microsoft Exchange Server 2007	Service Packs for Microsoft Exchange 2007 (SP1).
Microsoft Exchange Server 2010	Service Packs for Microsoft Exchange 2010 (SP1).

Component	Install Compatible Version
Microsoft Exchange Server 2013	Service Packs for Microsoft Exchange 2013 (SP1).
Active Directory	• Active Directory 2003 with Windows Server 2003 (SP2) • Active Directory 2008 with Windows Server 2008 (SP2) **Note** User names configured in Active Directory must be identical to those names defined in 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 Presence Service supports certificates using RSA 1024 or 2048 bit keys and SHA1 and SHA256 signature algorithms.

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

Configuration Considerations

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 47 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 52.

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

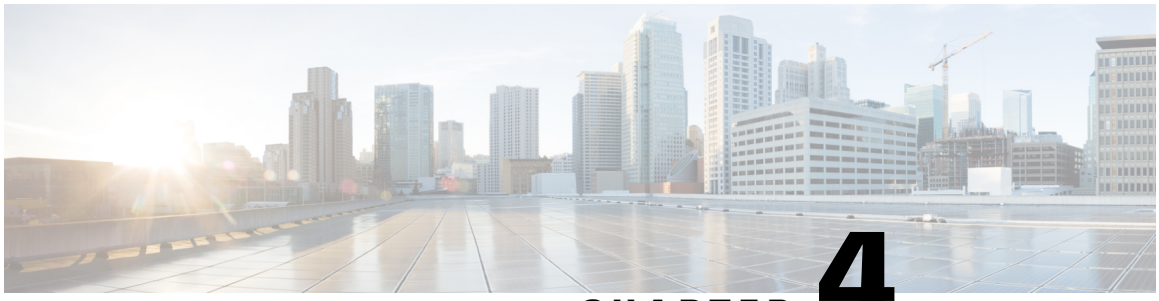
http://technet.microsoft.com/en-us/library/bb124558.aspx

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 4

Integrate Microsoft Exchange with the IM and Presence Service over Exchange Web Services

- Microsoft Exchange 2007 Configuration over Exchange Web Services, page 13
- Microsoft Exchange 2010 and 2013 Configuration over Exchange Web Services, page 19
- Enable Authentication on the Exchange Virtual Directories, page 26

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 14
- Grant Users Permission to Sign in to the Service Account Locally, on page 14
- Setting Impersonation Permissions at the Server Level , on page 16
- Granting Send As Permissions to the Service Account and User Mailboxes, on page 17
- Granting Impersonation Permissions to the Service Account and User Mailboxes, on page 18
- Verifying Permissions on the Microsoft Exchange 2007 Account, on page 19

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 16

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 16

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 17

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 17

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 18

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 19

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.

Before You Begin

Delegate the appropriate permissions to the Exchange 2007 account. See, Microsoft Exchange 2007 Configuration over Exchange Web Services, on page 13.

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 th e 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 26

Microsoft Exchange 2010 and 2013 Configuration over Exchange Web Services

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

- Verifying Windows Security Settings
- Setting Exchange Impersonation Permissions for Specific Users or Groups
- Verify Permissions on the Microsoft Exchange 2010 Accounts, on page 24

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 3: 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 requests to the Client Access Server (CAS), we recommend that you increase this parameter to 100.

Table 4: Recommended Throttle Policy Settings on Exchange Server 2013

Parameter[1]	Recommended Configuration Value — Exchange Server 2013
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, on page 23.

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 defined in Microsoft Exchange 2010 and 2013 Configuration over Exchange Web Services, on page 19.

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
```

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 24

Related Topics

Exchange Server 2010
Exchange Server 2013

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

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. 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 21.

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

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*

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 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 Accounts, on page 25.

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	RoleAssigneeName	RoleAssigneeType	AssignmentMethod	EffectiveUserName
_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- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

Step 5 Verify that the ThrottlingPolicy parameters match what is defined in Microsoft Exchange 2010 and 2013 Configuration over Exchange Web Services, on page 19 by running this command in the EMS.

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

What to Do Next

Enable Authentication on the Exchange Virtual Directories, on page 26

Related Topics

Exchange Server 2010
Exchange Server 2013

Verify Permissions on the Microsoft Exchange 2013 Accounts

After you have assigned the permissions to the Exchange 2013 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 2013, it takes some time for the permissions to propagate to mailboxes.

These are the commands for Exchange Server 2013. If you are using Exchange Server 2010, follow the steps in Verify Permissions on the Microsoft Exchange 2010 Accounts, on page 24.

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 XREF by running this command in the EMS.

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

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 a Presence Gateway for Microsoft Exchange Integration , on page 29

Enable Authentication on Exchange 2010 and 2013 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**

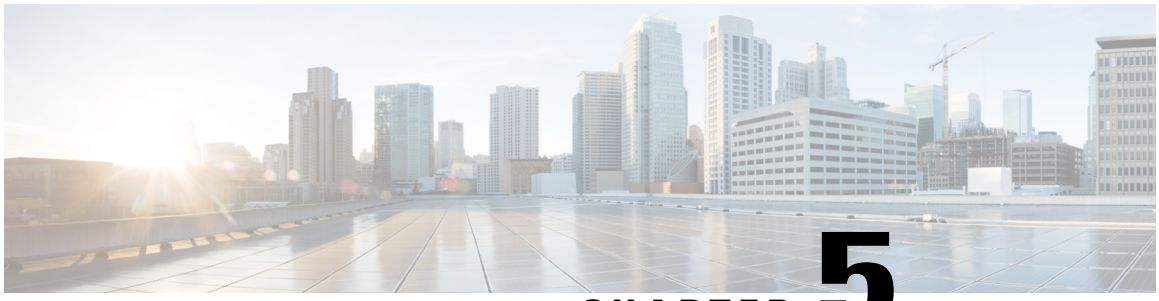
Step 7 Use the **Enable/Disable** link in the Actions column to configure appropriately.

What to Do Next

Configure a Presence Gateway for Microsoft Exchange Integration , on page 29

Related Topics

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



CHAPTER 5

Configure the IM and Presence Service to Integrate with the Microsoft Exchange Server

- Configure a Presence Gateway for Microsoft Exchange Integration , page 29
- SAN and Wildcard Certificate Support, page 31
- Configure Secure Certificate Exchange Between the IM and Presence Service and Microsoft Exchange, page 32
- Enabling Calendar Integration, page 42
- [Optional] Configure the Frequency of Exchange Calendar Notifications Sent Over Exchange Web Services, page 43
- [Optional] Configure the Microsoft Exchange Notification Port , page 44
- [Optional] Configuring the Duration Range of Microsoft Exchange Calendar Notifications, page 45
- Other Microsoft Exchange Calendaring Parameters, page 46

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 47.
- 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 48.

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 32
- Installing a CA on Windows Server 2008, on page 33

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 34

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 35

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 36

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 36

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 37

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 38

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 39

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 39

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 40

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 Cisco Unified 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**).	1 Log in to the **Cisco Unified CM IM and Presence Administration** user interface. 2 Choose **System** > **Security** > **Certificate Import Tool**. 3 Choose **IM and Presence(IM/P) Trust** as the Certificate Trust Store where you want to install the certificates. This stores the Presence Engine trust certificates required for Exchange integration. 4 Enter one of these values to connect with the Exchange Server: • IP address • Hostname • FQDN The value that you enter in this Peer Server field must exactly match the IP address, hostname or FQDN of the Exchange Server. 5 Enter the port that is used to communicate with the Exchange Server. This value must match the available port on the Exchange Server. 6 Click **Submit**. After the tool finishes, it reports these states for each test: • Peer Server Reachability Status — indicates whether or not the IM and Presence Service can reach (ping) the Exchange Server. See Troubleshooting Exchange Server Connection Status, on page 47. • SSL Connection/Certificate Verification Status — indicates whether or not the Certificate Import Tool succeeded in downloading certificates from the specified peer server and whether or not a secure connection has been established between the IM and Presence Service and the remote server. See Troubleshooting SSL Connection Certificate Status , on page 48.

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**).	1 Copy or FTP the **certnew.cer** certificate file to the computer that you use to administer your IM and Presence Service node. 2 Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. 3 Choose **Security** > **Certificate Management**. 4 In the **Certificate List** window, choose **Upload Certificate/Certificate Chain**. 5 Complete these actions when the **Upload Certificate/Certificate Chain** dialog box opens: • From the Certificate Name drop-down list, choose **cup-trust**. • Enter the root certificate name without any extension. 6 Click **Browse** and choose **certnew.cer**. 7 Click **Upload File**.

Step 3 Return to the Certificate Import Tool (Step 1, on page 40) and verify that all status tests succeed.

Step 4 Restart the Cisco Presence 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).

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 29.

Enabling Calendar Integration for Individual Users

Procedure

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

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

Step 3 In the Service Settings area, check the check box for Include meeting information in presence (requires an Exchange Presence Gateway to be configured on the Cisco Unified Communications Manager IM and Presence Service node).

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**.

Step 3 In the appropriate Users area, choose a File Name.

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

Step 4 Click **Run Immediately** or **Run Later**.

Step 5 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**.

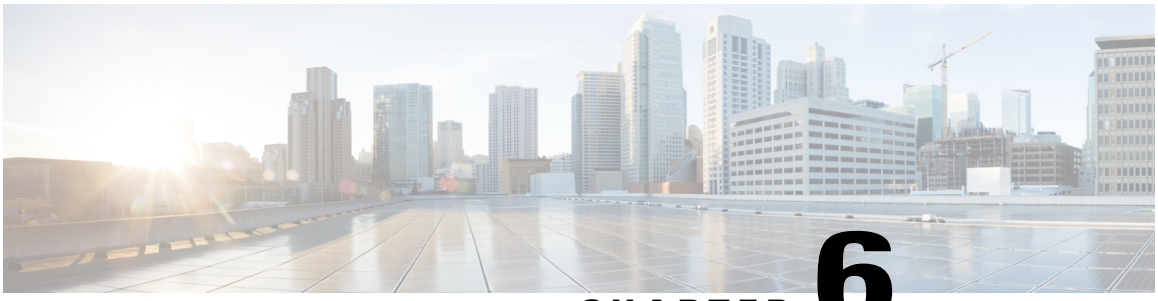
Tip If a very large number of users transition either in or out of meetings, a mass notification event occurs that may delay some notifications up to a few minutes.

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 6

Troubleshooting Exchange Calendaring Integrations

- Troubleshooting Exchange Server Connection Status, page 47
- Troubleshooting SSL Connection Certificate Status , page 48
- Issues Known to Impact Microsoft Exchange Integrations , page 52

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 Exchange Server.

Test	Status Description and Recommended Action
Exchange Reachability (unreachable)	The IM and Presence Service failed to ping the Exchange Server. The server may not be reachable due to an incorrect field value or an issue with the customer's network, for example, cabling. To resolve this, ensure that the Presence Gateway field contains the correct value (FQDN or IP address) to reach the Exchange Server over the network. Note that the UI does not require the Presence Gateway field value to be the Subject CN value. If you have connection problems with the Exchange Server, also see the System Troubleshooter in **Cisco Unified CM IM and Presence Administration** and implement the recommended solution. Choose **Diagnostics** > **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 Exchange Server. Click **View** for the certificate details.

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**.	

Test	Status Description and Recommended Action
	One or more certificates that the IM and Presence Service requires to establish a secure connection to the Exchange Server are missing. The Certificate Viewer can provide details of the missing certificates. Complete these steps in the Certificate Viewer to display any missing certificates: **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 status of Missing. **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 use to administer the IM and Presence Service. **3** Use **Cisco Unified IM and Presence OS Administration** to upload any of the required missing certificates. **Troubleshooting Tips** • If the certificates are not available in the Certificate Viewer, you may need to manually download and install the missing certificates from the Exchange Server, and upload these certificates in **Cisco Unified IM and Presence OS Administration** as follows: ◦ Log in to the **Cisco Unified IM and Presence OS Administration** and user interface and upload certificates to complete the certificate chain. ◦ Return to the **Presence Gateway Configuration** window under the **Cisco Unified CM IM and Presence Administration** user interface, reopen the Certificate Viewer, and verify that all certificates in the certificate chain now have a status of Verified. • You must restart the Cisco Presence Engine after you upload Exchange trust certificates. • Log in to **Cisco Unified IM and Presence Serviceability** user interface. • Choose **Tools** > **Service Activation**. Note that this can affect Calendaring connectivity. • Choose either **Configure** or **View** to launch the Certificate Chain Viewer. The **Configure** button displays if there are any issues with the certificate chain that the IM and Presence Service downloads from the Exchange Server. For example, the missing certificates scenario described above. Once you successfully import and verify the certificate chain, the SSL

Test	Status Description and Recommended Action
	Connection / Certificate Verification status updates to Verified and the **View** button replaces **Configure**.
SSL Connection/Certificate Verification Failed-Subject CN Mismatch	The Presence Gateway field value must match the Subject CN value of the leaf certificate in the Certificate Chain. You can 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. The IM and Presence Service uses the Presence Gateway field value to ping the server. The host (FQDN or IP address) that you enter must exactly match the IIS certificate Subject Common Name. **2** Click **Save**. **Tip** Choose either **Configure** or **View** to launch the Certificate Chain Viewer. The **Configure** button displays if there are any issues with the certificate chain downloaded from the Exchange Server. For example, the missing certificates scenario described above. Once you successfully import and verify the certificate chain, the SSL Connection / Certificate Verification status updates to Verified and the **View** button replaces **Configure**.
SSL Connection/Certificate Verification Failed - SAN Mismatch	The Presence Gateway field value must match one of the Subject Alternative Name (SAN) values of the leaf certificate in the Certificate Chain. You can 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 SAN value in the Presence Gateway field. The IM and Presence Service uses the Presence Gateway field value to ping the server. The host (FQDN or IP address) that you enter must exactly match one of the entries in the certificate Subject Alternative Name. **2** Click **Save**. **Tip** Choose either **Configure** or **View** to launch the Certificate Chain Viewer. The **Configure** button displays if there are any issues with the certificate chain downloaded from the Exchange Server. For example, the missing certificates scenario described above. Once you successfully import and verify the certificate chain, the SSL Connection / Certificate Verification status updates to Verified and the **View** button replaces **Configure**.

Test	Status Description and Recommended Action
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 not the public key. This could happen if the Exchange Server regenerates the certificate but the IM and Presence Service node still maintains the old certificate. 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 certificate from the IM and Presence Service in Cisco Unified IM and Presence OS Administration, and then upload a new certificate in Cisco Unified IM and Presence OS Administration. • If the error is due to an unsupported algorithm, you need to upload a new certificate that contains the supported algorithm in Cisco Unified 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 Presence Service cannot verify the SSL connection. We recommend that you verify the network connectivity to the Exchange Server, and ensure that the Exchange Server is 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 Service cannot perform the reachability test. 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 5: Scale Limitations for Specific Cisco Unified Presence Releases

Software Release	% of Users Subscribing to Calendar Presence	% of Users Performing Simultaneous Calendar Transitions
8.5(1)	50	30

Software Release	% of Users Subscribing to Calendar Presence	% of Users Performing Simultaneous Calendar Transitions
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 Cisco Unified Communications Manager and user authentication on client applications subsequently fails. However, it has been observed during testing that once Cisco Unified 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 Cisco Unified 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 Cisco Unified 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.