Planning for Calendar Integration

- Prerequisites, on page 1
- Configuration Considerations, on page 2
- Security Considerations, on page 4
- Getting More Information , on page 4

Prerequisites

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

Table 1: Compatibility Matrix

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

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

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

Configuration Considerations

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

Table 2: Configuration Tasks for Microsoft Deployments

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

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 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.

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