CHAPTER 1

Planning for Cisco Unified Presence Integration with Microsoft Exchange

Revised: November 30, 2012

Microsoft Exchange Calendaring States on Cisco Unified Presence

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

Table 1-1 Aggregated Availability State Based on Calendar State

Microsoft Outlook State	Cisco Unified Presence State
Free/Tentative	Available
Busy	Idle/Busy
Out-of-Office[1] Away[2]	Away

1. Microsoft Oulook 2003 and 2007

2. Microsoft Outlook 2010

Presence Gateway Options

You must configure a Microsoft Exchange server (Microsoft Outlook) as a presence gateway for calendaring information exchange. The Exchange gateway enables the Cisco Unified Presence server to reflect the availability information (calendar/meeting status) in the availability status of the user on a per-user basis.

When you configure the presence gateway, you can use one of the following values to connect with the Microsoft Exchange server:

- FQDN
- IP address

Windows Security Policy Settings

Cisco Unified Presence integration with Exchange supports various authentication methods including Windows Integrated authentication (NTLM).

Note Cisco Unified Presence supports NTLMv1 Windows Integrated authentication only and does not currently support NTLMv2.

Some Windows network security policies allow NTLMv2 authentication only, which will prevent the integration between Cisco Unified Presence and Exchange from functioning (both WebDAV and EWS). You must verify that NTLMv2 authentication is not enabled on each Windows server running Exchange. If NTLMv2 authentication is enabled, disable the setting and reboot the server to properly apply the new security setting.

Complete the following procedure to verify the current value of NTLM authentication and if necessary, to disable NTLMv2 authentication.

Step 1 Select **Start > Administrative Tools > Local Security Policy** on the Windows server running Exchange.

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

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

Step 4 Verify that the **Require NTLMv2 session security** checkbox is not checked.

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

a. Uncheck the **Require NTLMv2 session security** checkbox.

b. Select **OK**.

Step 6 Reboot the Windows server running Exchange to apply the new security settings.

Certificate Support

Cisco Unified Presence uses X.509 certificates for secure authentication in calendaring integration with Microsoft Exchange.

From Release 8.6(4) onwards, Cisco Unified Presence supports SAN (Subject Alternative Name) and wildcard certificates, along with standard certificates. For information about certificate compatibility for Cisco Unified Presence Release 8.6(3) and earlier, see SAN and Wildcard Certificate Compatibility - Pre Release 8.6(4), page 1-3.

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

Note For SAN certificates, the protected host must be contained in the list of host names/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.

Wildcard certificates allow a domain and unlimited sub-domains to be protected 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 Wildcards can be placed in the Common Name (CN) for standard certificates, and in the Subject Alternative Name for SAN certificates.

SAN and Wildcard Certificate Compatibility - Pre Release 8.6(4)

Cisco Unified Presence uses X.509 certificates for secure authentication in calendaring integration with Microsoft Exchange. Cisco Unified Presence only supports standard certificates (no Subject Alternative Name field or wildcard entries); however, it is still possible to use SAN and/or Wildcard certificates for WebDAV and EWS calendaring integrations with Microsoft Exchange.

Note When using SAN/Wildcard certificates, there are some scenarios where the **Exchange Server Status** on the **Presence Gateway Configuration** page will report a **Subject CN Mismatch**, but calendaring integration continues to work.

Table 1-2 lists and describes the certificate types that Cisco Unified Presence supports for calendaring integration with Microsoft Exchange.

Table 1-2 Cisco Unified Presence SAN and Wildcard Certificates—Backwards Compatibility

X.509 Certificate Type	Description	Caveats
Standard	Presence gateway hostname/IP address contained in **Subject Common Name**.	None
Standard/Wildcard	Presence gateway subdomain wildcard contained in **Subject Common Name**.	**Presence Gateway Configuration Exchange Server Status** reports Subject CN Mismatch error.
SAN	Presence gateway hostname/IP address contained in both **Subject Common Name** and **Subject Alternative Name**.	None
SAN	Presence gateway hostname/IP address contained in **Subject Alternative Name** only.	**Presence Gateway Configuration Exchange Server Status** reports **Subject CN Mismatch** error.
SAN/Wildcard	Presence gateway subdomain wildcard contained in **Subject Alternative Name** only.	**Presence Gateway Configuration Exchange Server Status** reports **Subject CN Mismatch** error.

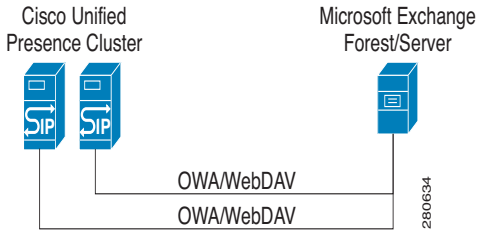
About Cisco Unified Presence Integration with Microsoft Exchange 2003 and 2007 - over WebDAV

Overview of Exchange Integration over the WebDAV Interface

Microsoft Exchange server (2003 and 2007 versions) support WebDav-based calendar integration.Figure 1 shows how the Microsoft Exchange server (2003 and 2007 versions) integrates with Cisco Unified Presence using the Outlook Web Access (OWA) protocol, over a WebDAV interface exposed by the Exchange server.

Cisco Unified Presence can only communicate with a single WebDav front-end Exchange server. The Exchange front-end server communicates with multiple Exchange back-end servers that you configure during the Webdav setup. Microsoft Exchange communicates with Cisco Unified Presence via a Presence Gateway configured for the Exchange server on Cisco Unified Presence.

Figure 1 Microsoft Exchange Integration with Cisco Unified Presence Architecture



Administrative Roles and Permissions in Exchange 2003 and 2007

By default in Microsoft Exchange 2003 and 2007, administrators are denied permission to sign into a user mailbox on the Exchange server. In order for Cisco Unified Presence to connect to mailbox stores on the Exchange server and query end-user calendaring data, it requires an Exchange account with special permissions, referred to as a 'receive-as' account.

What To Do Next

Chapter 2, "Configuring Microsoft Exchange Server 2003 and 2007 for Integration with Cisco Unified Presence (over WebDAV)."

Known Issues with this Integration

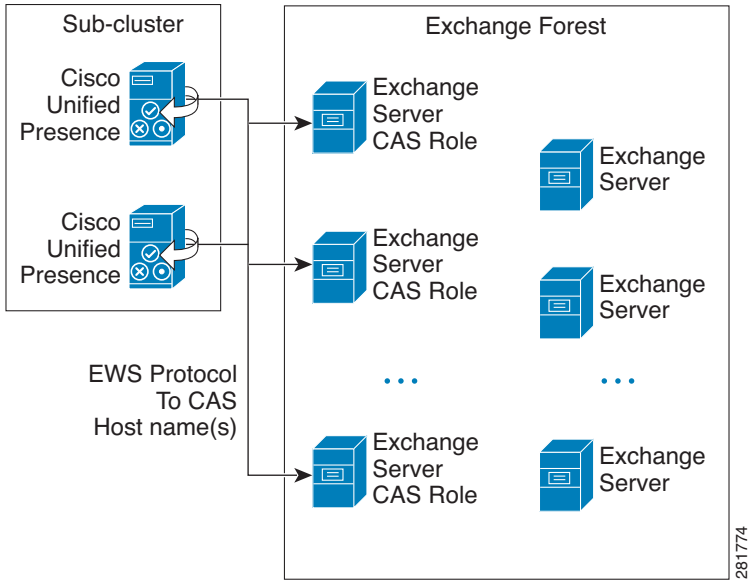
See the Troubleshooting section of this guide to learn about issues that are known to impact WebDAV integrations. See Issues Known to Impact Microsoft Exchange Integrations, page 6-5.

About Cisco Unified Presence Integration with Microsoft Exchange 2007 and 2010 - over Exchange Web Services (EWS)

Overview of Exchange Integration over the EWS Interface

In addition to WebDAV integration, Microsoft Exchange 2007 introduces Exchange Web Services (EWS) for calendaring integration using a SOAP-like interface to the Exchange server. For Microsoft Exchange 2010, WebDAV is no longer supported and customers can only use EWS for calendaring integration.

Note The Meeting Notification and Cisco IP Phone Messenger features will only work if your Exchange integration is with Microsoft Exchange 2003 or 2007 over WebDAV. Note that the "Today's Meeting" setting on Cisco IP Phone Messenger will not work with an EWS integration.



Administrative Roles and Permissions in Exchange Server 2007 and 2010

Just as WebDAV access requires a special account to enable access to all users accounts, EWS requires a similar capability. EWS manages this capability by assigning a "role" to a designated account. This role has the impersonation permission.

Microsoft Exchange Server 2007

For a caller to access the email account of another user on an Exchange 2007 server, 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** right on the Client Access Server (CAS) running Exchange 2007. This gives the caller the permission to impersonate a user email account using the CAS server. In addition, the caller must be granted the **ms-Exch-EPI-MayImpersonat**e right 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

Microsoft Exchange Server 2010 uses 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 or 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 which 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 Microsoft Exchange Server 2007 and 2010 Integrations

To support a large number of users (with EWS calendar integration enabled), Cisco Unified Presence must distribute the load of EWS traffic among multiple CAS servers. Cisco Unified Presence can connect to a number of CAS servers via EWS, and it uses this 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 server from the pool of eligible CAS hosts.
- Each CAS requires its own intermediate certificate so that Cisco Unified Presence can trust the intermediate certificate chain.

Note This release of Cisco Unified Presence does not support the Microsoft Exchange autodiscover service. The autodiscover service assumes that a load-balancing mechanism is already in place across the CAS servers.

When configuring your EWS presence gateway for Exchange integration in Cisco Unified Presence Administration, note the following:

- You cannot deploy a mixed environment of WebDAV and EWS servers. You must either configure a single WebDAV server or one or more EWS server gateways but not both.
- 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.

- 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 UP 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 UP Presence Engine once to effect all your changes simultaneously.

What To Do Next

Chapter 3, "Configuring Microsoft Exchange Server 2007 and 2010 for Integration with Cisco Unified Presence (over EWS)."

Known Issues with this Integration

Any issues that are known to impact EWS integrations are documented in the Troubleshooting section of this guide.

See Issues Known to Impact Microsoft Exchange Integrations, page 6-5.

Prerequisite Configuration Tasks

Before you configure Microsoft Exchange integration with Cisco Unified Presence, consult the compatiblity matrix below and make sure that you have installed and configured the required components for this integration:

Table 1-3 Compatibility Matrix

Component	Install Compatible Version
Windows Server	• Latest Service Packs for Windows Server 2003 (SP2) • Latest Service Packs for Windows Server 2008 (SP2)
Cisco Unified Communications Manager	Release 6.x or a higher release
Cisco Unified Presence	Release 8.5 or higher
Microsoft Exchange Server 2003	Latest Service Packs for Microsoft Exchange 2003 (SP2)
Microsoft Exchange Server 2007	Latest Service Packs for Microsoft Exchange 2007 (SP1).
Microsoft Exchange Server 2010	Latest Service Packs for Microsoft Exchange 2010 (SP1).

Component	Install Compatible Version
Active Directory	• Active Directory 2003 with Windows Server 2003 (SP2) -- OR -- • 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.

Related Topics

Use the Cisco Unified Presence User Options pages to configure calendaring states on client applications.

Getting More Information

Cisco Unified Presence Documentation

http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

Cisco Unified Communications Manager Documentation

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

Microsoft Exchange 2003 Documentation

http://technet.microsoft.com/en-us/library/bb123872.aspx

Microsoft Exchange 2007 Documentation

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

- For more information about how to configure FBA for Outlook web access in Exchange 2007, see the following URL:

  http://technet.microsoft.com/en-us/library/aa998867(EXCHG.80).aspx

Microsoft Exchange 2010 Documentation

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

Microsoft Active Directory Documentation

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