Configuring Microsoft Exchange Server 2007 and 2010 for Integration with Cisco Unified Presence (over EWS)

Revised: November 28, 2013

This module describes the integration of Cisco Unified Presence with Exchange Server 2007 and 2010 **over Exchange Web Services (EWS)**. If you are integrating with the Exchange Server 2003 or 2007 over WebDAV, see Chapter 3, "Configuring Microsoft Exchange Server 2003 and 2007 for Integration with Cisco Unified Presence (over WebDAV)."For an overview of each type of Exchange integration, we recommend that you review Chapter 2, "Planning for Cisco Unified Presence Integration with Microsoft Exchange".

Microsoft Exchange 2007 Configuration (EWS)

Before You Begin

Note that the steps required to configure Exchange Server 2007 are different, depending on whether you use Windows Server 2003 or Windows Server 2008. For detailed instruictions see the Exchange Server 2007 documentation at http://technet.microsoft.com/?en-us/?library/?bb124558(EXCHG.80).aspx.

You must complete the following tasks when configuring access to mailboxes on Exchange Server 2007.

- Verify the Windows Security Policy Settings
- Grant Users Permission to Log on to the Service Account Locally
- Set Impersonation Permissions at the Server Level
- Set Active Directory Service Extended Permissions for the Service Account
- Grant Send As Permissions to the Service Account and User Mailboxes
- Grant Impersonation Permissions to the Service Account and User Mailboxes

For detailed instructions, see the Exchange Server 2007 documentation at the following URL: http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx

Verify the Windows Security Policy Settings

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

Follow this procedure to ensure NTLMV2 is not enabled.

Procedure

Step 1 On the Windows Server 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** checkbox is not checked.

Step 5 Complete the following steps if the **Require NTLMv2 session security** checkbox is checked:

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

b. Click **OK**.

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

What To Do Next

Grant Users Permission to Log on to the Service Account Locally

Grant Users Permission to Log on to the Service Account Locally

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

Before you begin

- For Exchange impersonation to work, all 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.

Exchange 2007 Configuration on Windows Server 2003

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 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** and 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**.

Exchange 2007 Configuration 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 Click **Start**.

Step 3 Type **gpmc.msc**

Step 4 Click **Enter**.

Step 5 On the Exchange Server, open the Domain Controller Security Settings window.

Step 6 In the left pane, under **Sccurity 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 selected.

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

Step 10 Click **OK**.

Step 11 Choose **Check Names**, and verify that the specified user is correct.

Step 12 Click **OK**.

Step 13 In the Allow Log On Locally Properties dialog box, click **Apply** and click **OK**.

Step 14 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

Set Impersonation Permissions at the Server Level

Set 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

To grant the service account rights to access individual Exchange servers, you may replace **Get-OrganizationConfig** with the string **Get-ExchangeServer -Identity** *server_name*, where *server_name* 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 the 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

Set Active Directory Service Extended Permissions for the Service Account

Set Active Directory Service Extended Permissions for the Service Account

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

Before you begin

- If the CAS is located behind a load-balancer, grant the **ms-Exch-EPI-Impersonation** rights to the Ex2007 account for *all* CAS behind the load-balancer.
- If your mailbox servers are located on a different machine to the CAS, grant **ms-Exch-EPI-Impersonation** rights for the Ex2007 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 In the EMS, run this Add-ADPermission command to add the impersonation permissions on the server for the identified service acccount (for example, Ex2007).

```
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 In the EMS, run this Add-ADPermission command 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

Grant Send As Permissions to the Service Account and User Mailboxes

Grant 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 Exchange Management Console (EMC) to complete this step.

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 In the EMS, run this Add-ADPermission command to grant Send As permisisons 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

Grant Impersonation Permissions to the Service Account and User Mailboxes

Grant Impersonation Permissions to the Service Account and User Mailboxes

Follow this procedure to grant Impersonation permission to the service account and user mailboxes.

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

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 In the EMS, run this Add-ADPermission command to grant Impersonation permission on the service account all associated mailbox stores:

```
Syntax
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishdName -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 Cisco Unified Presence only requires Impersonation permissions on the account to enable it to sign in to that account when it connects to the Exchange Server. Note that this account does not typically receive mail so space does not need to be allocated for it.

What To Do Next

Verifying Permissions on the Exchange 2007 Account, page 4-6

Verifying Permissions on the Exchange 2007 Account

After you have assigned the permissions to the Exchange 2007 account, you must verify that the permissions propagate to mailbox level and that a selected 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 account. See the Exchange 2007 Configuration (EWS) topic. Microsoft Exchange 2007 Configuration (EWS)

Procedure

Step 1 In the console tree of the EMC on the Exchange Server 2007, right-click **Active Directory Sites and Services**.

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

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

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

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 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 have 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

How to Enable Authentication on the Exchange 2007/2010 Virtual Directories, page 4-10.

Microsoft Exchange 2010 Configuration (EWS)

Follow the below tasks when configuring access to mailboxes on the Exchange Server 2010.

- Verifying Windows Security Settings
- Set Exchange Impersonation Permissions for Specific Users or Groups of Users

For detailed instructions, see the Exchange Server 2010 documentation at the following URL: http://technet.microsoft.com/en-us/library/bb124558.aspx

Before You Begin

Before you integrate Exchange Server 2010 with Cisco Unified Presence over EWS, ensure that you configure the following throttle policy parameter values on the Exchange Server. These are the values that are required for the EWS calendaring integration with Cisco Unified Presence to work.

Note You do not have to modify the default throttling policy settings. A new policy can be created with the recommended values in the table.

Table 4-1 Recommended Throttle Policy Parameter Values on Microsoft Exchange

Parameter	Recommended Configuration Value
EWSMaxConcurrency	It has been observed during Cisco tests that the default throttling policy value is sufficient to support 50% calendaring-enabled users. If you have a higher load of EWS requests to the Client Access Server (CAS), however, we recommend that you increase this parameter to 100.
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60
EWSMaxSubscriptions	NULL

Parameter	Recommended Configuration Value
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000

Verifying Windows Security Settings

Cisco Unified Presence supports NTLMv1 Windows Integrated authentication only, and does not currently support NTLMv2. Complete this procedure to ensure that NTLMV2 is not enabled.

Procedure

Step 1 On the Windows Server 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** checkbox is not checked.

Step 5 Complete the following steps if the **Require NTLMv2 session security** checkbox is checked:

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

b. Click **OK**.

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

Set Exchange Impersonation Permissions for Specific Users or Groups of Users

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

Procedure

Step 1 Create the account in Active Directory.

Step 2 Open the EMS for command line entry.

Step 3 In the EMS, run the New-ManagementRoleAssignment command to grant a specified 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 permisisons 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 Table 4-1.

```
Syntax
New-ThrottlingPolicy -Name:Policy_Name -EWSMaxConcurrency:100 -EWSPercentTimeInAD:50
-EWSPercentTimeInCAS:90 -EWSPercentTimeInMailboxRPC:60 -EWSMaxSubscriptions:NULL
-EWSFastSearchTimeoutInSeconds:60 -EWSFindCountLimit:1000

Example
New-ThrottlingPolicy -Name:CUPThrottlingPolicy -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
cup_throttling_policy
```

What To Do Next

Verifying Permissions on the Exchange 2010 Account, page 4-9

Related Topics

For a complete description of the Exchange Server 2010 parameters, see http://technet.microsoft.com/en-us/library/dd351045.aspx

Verifying Permissions on the Exchange 2010 Account

After you have assigned the permissions to the Exchange 2010 account, you must verify that the permissions propagate to mailbox level and that a selected 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.

Before You Begin

Complete the steps in the Exchange 2010 Configuration topic. Microsoft Exchange 2010 Configuration (EWS), page 4-7.

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. In the EMS, run this command:

```
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	RoleAssignee Type	Assignment Method	EffectiveUser Name
_suImpersonate RoleAsg	Application Impersonation	ex2010	User	Direct	ex2010

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

a. In the EMS, run this command:

```
Get-ManagementScope _suImpersonateScope
```

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

Example: Command Output

Name	ScopeRestrictionType	Exclusive	RecipientRoot	Recipient Filter	ServerFilter
_suImpersonate Scope	ServerScope	False			Distinguished Name

Step 5 Verify that the ThrottlingPolicy parameters match what is defined in Table 4-1 by running this command.

a. In the EMS, run this command:

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

What To Do Next

How to Enable Authentication on the Exchange 2007/2010 Virtual Directories, page 4-10

How to Enable Authentication on the Exchange 2007/2010 Virtual Directories

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

- Enabling Authentication on Exchange 2007 Running Windows Server 2003, page 4-11
- Enabling Authentication on Exchange 2010 Running Windows Server 2008, page 4-11

Enabling Authentication on Exchange 2007 Running Windows Server 2003

Complete the following procedure to enable authentication on Exchange 2007 running Windows Server 2003.

Procedure

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

Step 2 Choose **Web Sites**.

Step 3 Choose **Default Web Site**.

Step 4 Right-click the **EWS** directory folders, 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 one or 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

Configuring the Presence Gateway on Cisco Unified Presence for Microsoft Exchange Integration, page 5-1

Enabling Authentication on Exchange 2010 Running Windows Server 2008

Complete the following procedure to enable authentication on Exchange 2010 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 area, choose **Authentication**.

Step 6 Verify that the following Authentication methods are enabled:

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

Step 7 In the Actions column, use the **Enable/Disable** link to configure appropriately.

What To Do Next

Configuring the Presence Gateway on Cisco Unified Presence for Microsoft Exchange Integration, page 5-1

Related Topics

- http://technet.microsoft.com/en-us/library/aa998849.aspx
- http://technet.microsoft.com/en-us/library/ee633481.aspx