Configure Microsoft Exchange

Microsoft Exchange Configuration for Calendar Integration

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

Table 1: Microsoft Exchange Configuration for Calendar Integration with the IM and Presence Service

Microsoft Exchange Deployment	Microsoft Configuration
Microsoft Exchange 2007	Microsoft Exchange 2007 Configuration Task Flow, on page 1
Microsoft Exchange 2010, 2013 or 2016	Microsoft Exchange 2010/2013/2016 Configuration Task Flow, on page 8

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

Microsoft Exchange 2007 Configuration Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Verifying Windows Security Settings	Verify Windows Security Settings such as your NTLM requirements.
Step 2	Configure the Exchange server to grant users the right to sign in locally: • Configuring Microsoft Exchange 2007 on Windows Server 2003 • Configuring Microsoft Exchange 2007 on Windows Server 2008	**Note** For Exchange impersonation to work, all Microsoft Exchange servers must be members of the Windows Authorization Access Group The service account should not be a member of any of the Exchange Administrative Groups. Exchange explicitly denies Impersonation for all accounts in those groups.
Step 3	Setting Impersonation Permissions at the Server Level	Grant permissions at the server, database, user, and contact levels.
Step 4	Setting Active Directory Service Extended Permissions for the Service Account	You must set permissions on the Client Access Server (CAS) for the service account that performs the impersonation.
Step 5	Granting Send As Permissions to the Service Account and User Mailboxes	Grant send as permissions to the service account and user mailboxes.
Step 6	Granting Impersonation Permissions to the Service Account and User Mailboxes	Grant impersonation permissions to the service account and user mailboxes.
Step 7	Verifying Permissions on the Microsoft Exchange 2007 Account	Verify that the permissions propagate to the mailbox level and that a specified user can access the mailbox and impersonate the account of another user.
Step 8	Enabling Authentication on Exchange 2007 Running Windows Server 2003	Enable authentication on the Exchange server.
Step 9	Configure Certificates for Exchange Server Task Flow , on page 17	Complete this task flow to configure certificates for a Microsoft Exchange deployment.

Verifying Windows Security Settings

Procedure

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

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

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

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

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

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

b) Click **OK**.

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

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

Configuring Microsoft Exchange 2007 on Windows Server 2003

Procedure

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

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

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

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

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

Step 6 Click **OK**.

What to do next

Setting Impersonation Permissions at the Server Level

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

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

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

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

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

Verifying Permissions on the Microsoft Exchange 2007 Account

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

Procedure

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

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

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

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

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

a) Your service account is listed.

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

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

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

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

What to do next

Enable Authentication on the Exchange Virtual Directories

Enabling Authentication on Exchange 2007 Running Windows Server 2003

Enabling Authentication on Exchange 2007 Running Windows Server 2003

Procedure

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

Step 2 Choose **Web Sites**.

Step 3 Choose **Default Web Site**.

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

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

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

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

- **Enable anonymous access**

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

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

Step 9 Click **OK**.

What to do next

Configure Certificates for Exchange Server Task Flow , on page 17

Microsoft Exchange 2010/2013/2016 Configuration Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Verify Windows Security Settings, on page 9	Verify your Windows Security Settings for Windows Integrated authentication (NTLM).

	Command or Action	Purpose
Step 2	Set Exchange permissions for your release: • Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2010 • Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2013 or 2016	Set the Exchange impersonation permissions for specific users or a group of users.
Step 3	Verify permissions for your release: • Verify Permissions on the Microsoft Exchange 2010 Accounts • Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts	Verify that the permissions propagate to the mailbox level and that a specified user can access the mailbox and impersonate the account of another user.
Step 4	Enable Authentication on Exchange 2010, 2013 or 2016 Running Windows Server 2008	Basic Authentication, Windows Integrated Authentication, or both must be enabled on the EWS virtual directory (/EWS) for the Exchange Server.
Step 5	Configure Certificates for Exchange Server Task Flow , on page 17	Complete this task flow to configure certificates for a Microsoft Exchange deployment.

Verify Windows Security Settings

Procedure

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

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

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

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

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

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

b) Click **OK**.

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

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

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

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

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

Procedure

Step 1 Create the account in Active Directory.

Step 2 Open the EMS for command line entry.

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

Syntax

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

Example

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

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

Syntax

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

Example

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

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

Syntax

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

Example

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

Table 2: Recommended Throttle Policy Settings on Exchange Server 2010

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

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

Note: Only available with supported Exchange SP1.

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

Syntax

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

Example

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

What to do next

Verify Permissions on the Microsoft Exchange 2010 Accounts

Related Topics

Exchange Server 2010
Exchange Server 2013

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

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

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

Procedure

Step 1 Create the account in Active Directory.

Step 2 Open the EMS for command line entry.

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

Syntax

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

Example

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

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

Syntax

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

Example

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

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

Syntax

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

Example

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

Table 3: Recommended Throttle Policy Settings on Exchange Server 2013 or 2016

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

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

Note: Only available with supported Exchange SP1.

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

Syntax

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

Example

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

What to do next

Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts

Verify Permissions on the Microsoft Exchange 2010 Accounts

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

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

Procedure

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

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

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

a) Run this command in the EMS:

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

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

Example Command Output

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

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

a) Run this command in the EMS:

```
Get-ManagementScope _suImpersonateScope
```

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

Example Command Output

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

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

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

Table 4: Recommended Throttle Policy Settings on Exchange Server 2010

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

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

What to do next

Enable Authentication on the Exchange Virtual Directories

Related Topics

Exchange Server 2010
Exchange Server 2013

Verify Permissions on the Microsoft Exchange 2013 or 2016 Accounts

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

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

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	ScopeRestrictionType	Exclusive	RecipientRoot	RecipientFilter	ServerFilter
_suImpersonateScope	ServerScope	False	User	Direct	DistinguishedName

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

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

Table 5: Recommended Throttle Policy Settings on Exchange Server 2013 or 2016

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

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

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

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

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

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

Procedure

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

Step 2 Choose **Web Sites**.

Step 3 Choose **Default Web Site**.

Step 4 Choose **EWS**.

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

Step 6 Verify that the following Authentication methods are enabled:

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

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

What to do next

Configure Certificates for Exchange Server Task Flow , on page 17

Related Topics

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

SAN and Wildcard Certificate Support

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

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

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

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

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

Configure Certificates for Exchange Server Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Install the Certificate Authority (CA) on your version of Windows Server: • Installing a CA on Windows Server 2003, on page 18 • Installing a CA on Windows Server 2008, on page 19	Although the Certificate Authority (CA) can run on the Exchange Server, we recommend that you use a different Windows Server as a CA to provide extended security for third-party certificate exchanges
Step 2	Generate a CSR for your version of Windows Server:: • Generating a CSR – Running Windows Server 2003 , on page 20 • Generating a CSR – Running Windows Server 2008 , on page 21	You must generate a Certificate Signing Request (CSR) on the IIS Server for Exchange, which is subsequently signed by the CA Server.
Step 3	Submitting a CSR to the CA Server/Certificate Authority, on page 22	We recommend that the default SSL certificate, generated for Exchange on IIS, should use the Fully Qualified Domain Name (FQDN) of the Exchange Server and be signed by a Certificate Authority that the IM and Presence Service

	Command or Action	Purpose
		trusts. This procedure allows the CA to sign the CSR from Exchange IIS.
Step 4	Downloading a Signed Certificate, on page 23	Download a copy of the signed certificate.
Step 5	Upload the signed certificate to your version of Windows Server • Uploading a Signed Certificate – Running Windows 2003, on page 24 • Uploading a Signed Certificate – Running Windows 2008, on page 25	This procedure takes the signed CSR and uploads it onto IIS.
Step 6	Downloading a Root Certificate, on page 25	Download a root certificate from your CA server.
Step 7	Upload a Root Certificate to the IM and Presence Service Node, on page 26	Upload the root certificate into the IM and Presence Service.

Installing a CA on Windows Server 2003

Before you begin

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

What to do next

Generating a CSR – Running Windows Server 2003 , on page 20

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 21

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 22

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 22

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 23

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

Upload a signed certificate for your server type:

- Uploading a Signed Certificate – Running Windows 2003, on page 24

• Uploading a Signed Certificate – Running Windows 2008, on page 25

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 25

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 25

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 26

Upload a Root Certificate to the IM and Presence Service Node

Before you begin

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

Procedure

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

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

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

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

Step 3 Return to the Certificate Import Tool (Step 1, on page 26) and verify that all status tests succeed.

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

Tips

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

What to do next

Configure the IM and Presence Service