Configure Microsoft Exchange for Calendaring Integration

- Microsoft Exchange 2007 Configuration over Exchange Web Services, on page 1
- Microsoft Exchange 2010 and 2013 Configuration over Exchange Web Services, on page 7
- Enable Authentication on the Exchange Virtual Directories, on page 16

Microsoft Exchange 2007 Configuration over Exchange Web Services

Before You Begin

Note that the steps required to configure Exchange Server 2007 differ depending on whether you use Windows Server 2003 or Windows Server 2008.

You must complete the following tasks when configuring access to mailboxes on the Exchange Server 2007. For detailed instructions, see the Exchange Server 2007 documentation at the following URL:http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx.

- Verifying Windows Security Settings, on page 2
- Grant Users Permission to Sign in to the Service Account Locally, on page 2
- Setting Impersonation Permissions at the Server Level , on page 4
- Granting Send As Permissions to the Service Account and User Mailboxes, on page 5
- Granting Impersonation Permissions to the Service Account and User Mailboxes, on page 6
- Verifying Permissions on the Microsoft Exchange 2007 Account, on page 7

Tip The IM and Presence Service only requires impersonation permissions on the account to enable it to log in to that account when it connects to the Exchange Server. Note that this account does not typically receive mail so you do not need to be concerned about allocating space for it.

Windows Security Policy Settings

IM and Presence Service integration with Microsoft Exchange supports various authentication methods including Windows Integrated authentication (NTLM).

IM and Presence Service supports both NTLMv1 and NTLMv2 Windows Integrated authentication, with NTLMv2 used as the default.

Configuring the **Lan Manager authentication level** to **Send NTLMv2 response only. Refuse LM & NTLM** on the Windows domain controller enforces NTLMv2 authentication on the domain.

Note IM and Presence Service does not support NTLMv2 session security. Message confidentiality and integrity are provided by secure http (https).

Verifying Windows Security Settings

Procedure

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

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

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

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

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

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

b) Click **OK**.

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

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

Grant Users Permission to Sign in to the Service Account Locally

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

Before you begin

- For Exchange impersonation to work, all Microsoft Exchange servers must be members of the Windows Authorization Access Group.
- The service account should not be a member of any of the Exchange Administrative Groups. Exchange explicitly denies Impersonation for all accounts in those groups.

Configuring Microsoft Exchange 2007 on Windows Server 2003

Procedure

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

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

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

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

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

Step 6 Click **OK**.

What to do next

Setting Impersonation Permissions at the Server Level , on page 4

Configuring Microsoft Exchange 2007 on Windows Server 2008

Procedure

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

Step 2 Choose Start.

Step 3 Type gpmc.msc.

Step 4 Choose Enter.

Step 5 Open the **Domain Controller Security Settings** window on the Exchange Server.

Step 6 In the left pane, under **Security Settings**, navigate to **Local Policies** > **User Rights Assignments**.

Step 7 In the right pane of the console, double-click **Allow Log On Locally**.

Step 8 Ensure that the **Define these policy settings** check box is checked.

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

Step 10 Choose **Check Names**, and verify that the specified user is correct. Then click **OK**.

Step 11 Click **Apply** then click **OK** in the **Allow Log On Locally Properties** dialog box.

Step 12 Determine if your users SMTP address is *alias@FQDN*. If it is not, you must impersonate using the user principal name (UPN). This is defined as *alias@FQDN*.

What to do next

Setting Impersonation Permissions at the Server Level , on page 4

Setting Impersonation Permissions at the Server Level

The command in the following procedure allows you to grant impersonation permissions at the server level. You can also grant permissions at the database, user, and contact levels.

Before you begin

- If you wish to only grant the service account rights to access individual Microsoft Exchange servers, replace

  Get-OrganizationConfig

  with the string

  Get-ExchangeServer -Identity *ServerName*

  where *ServerName* is the name of the Exchange Server.

  Example

  Add-ADPermission -Identity (Get-ExchangeServer -Identity *exchangeserver1*).
  DistinguishedName -User (Get-User -Identity *user* **| select-object).identity -ExtendedRights Send-As**

- Verify that the SMTP address of your users is defined as alias@FQDN. If it is not, you must impersonate the user account using the User Principal Name (UPN).

Procedure

Step 1 Open the Exchange Management Shell (EMS) for command line entry.

Step 2 Run this Add-ADPermission command to add the impersonation permissions on the server.

Syntax

Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity *User* **| select-object).identity -AccessRights GenericAll -InheritanceType Descendents**

Example

Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity *Ex2007* **| select-object).identity -AccessRights GenericAll -InheritanceType Descendents**

What to do next

Setting Active Directory Service Extended Permissions for the Service Account, on page 4

Setting Active Directory Service Extended Permissions for the Service Account

Before you begin

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

- If the CAS is located behind a load-balancer, grant the **ms-Exch-EPI-Impersonation** rights to the Microsoft Exchange 2007 account for all CASs behind the load-balancer.
- If your mailbox servers are located on a different machine to the CASs, grant **ms-Exch-EPI-Impersonation** rights for the Exchange 2007 account for all mailbox servers.
- You can also set these permissions by using **Active Directory Sites and Services** or the **Active Directory Users and Computers** user interfaces.

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this Add-ADPermission command in the EMS to add the impersonation permissions on the server for the identified service account (for example, Exchange 2007).

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

Step 3 Run this Add-ADPermission command in the EMS to add the impersonation permissions to the service account on each mailbox that it impersonates:

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

What to do next

Granting Send As Permissions to the Service Account and User Mailboxes, on page 5

Granting Send As Permissions to the Service Account and User Mailboxes

Follow this procedure to grant send as permissions to the service account and user mailboxes.

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

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this Add-ADPermission command in the EMS to grant Send As permissions to the service account and all associated mailbox stores:

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRights Send-As
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRights Send-As
```

What to do next

Granting Impersonation Permissions to the Service Account and User Mailboxes, on page 6

Granting Impersonation Permissions to the Service Account and User Mailboxes

Follow this procedure to grant impersonation permissions to the service account and user mailboxes.

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

Procedure

Step 1 Open the Exchange Management Shell (EMS).

Step 2 Run this **Add-ADPermission** command in the EMS to grant impersonation permissions on the service account all associated mailbox stores:

Syntax

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity User | select-object) .identity -ExtendedRights Receive-As
```

Example

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity EX2007 | select-object) .identity -ExtendedRights Receive-As
```

Note The IM and Presence Service only requires impersonation permissions on the account to enable it to log in to that account when it connects to the Exchange Server. This account does not typically receive mail so you do not need to be concerned about allocating space for it.

What to do next

Verifying Permissions on the Microsoft Exchange 2007 Account, on page 7

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, on page 16

Enabling Authentication on Exchange 2007 Running Windows Server 2003, on page 16

Microsoft Exchange 2010 and 2013 Configuration over Exchange Web Services

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

Before You Begin

Before you use Exchange Web Services (EWS) to integrate Exchange 2010 and 2013 servers with IM and Presence Service, ensure that you configure the throttle policy parameter values on the Exchange Server. These are the values that are required for the EWS calendaring integration to work with IM and Presence Service.

These are the commands and settings for Exchange Server 2010 and 2013.

Table 1: 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.

Table 2: 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.

Related Topics

Exchange Server 2010
Exchange Server 2013

Windows Security Policy Settings

IM and Presence Service integration with Microsoft Exchange supports various authentication methods including Windows Integrated authentication (NTLM).

IM and Presence Service supports both NTLMv1 and NTLMv2 Windows Integrated authentication, with NTLMv2 used as the default.

Configuring the **Lan Manager authentication level** to **Send NTLMv2 response only. Refuse LM & NTLM** on the Windows domain controller enforces NTLMv2 authentication on the domain.

Note IM and Presence Service does not support NTLMv2 session security. Message confidentiality and integrity are provided by secure http (https).

Verifying Windows Security Settings

Procedure

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

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

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

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

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

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

b) Click **OK**.

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

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

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

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

These are the commands and settings for Exchange Server 2010. If you are using Exchange Server 2013, follow the steps in Set Exchange Impersonation Permissions for Specific Users or Groups for Exchange 2013 or 2016 , on page 11.

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 3: Recommended Throttle Policy Settings on Exchange Server 2010

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

[1] During Cisco testing, the default throttling policy value was sufficient to support 50% calendaring-enabled users. However. if you have a higher load of EWS r 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, on page 13

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, on page 9.

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 4: 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, on page 14

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, on page 14.

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 Roc -
_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 5: 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.

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, on page 13.

Procedure

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

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

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

a) Run this command in the EMS:

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

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

```
Example Command Output
```

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	User	Direct	ex2010

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

a) Run this command in the EMS:

```
Get-ManagementScope _suImpersonateScope
```

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

Example Command Output

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

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

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

Table 6: 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.

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

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

Enable Authentication on the Exchange Virtual Directories

Before you begin

For the Exchange Web Services (EWS) integration to work properly, Basic Authentication, Windows Integrated Authentication, or both must be enabled on the EWS virtual directory (/EWS) for Exchange Server 2007, 2010, and 2013.

Enabling Authentication on Exchange 2007 Running Windows Server 2003

Procedure

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

Step 2 Choose **Web Sites**.

Step 3 Choose **Default Web Site**.

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

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

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

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

- **Enable anonymous access**

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

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

Step 9 Click **OK**.

What to do next

Configure Certificates for Exchange Server Task Flow

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

Related Topics

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