

Deployment Guide for the System Center Service Manager Exchange Connector 4.0

Microsoft Corporation

Published: August 2020

Applies To

Microsoft System Center 2016 Service Manager, Microsoft System 2019 Center Service Manager

Feedback

Send suggestions and comments about this document to systemcenterfeedback@microsoft.com.

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2015 Microsoft Corporation. All rights reserved.

Microsoft, ActiveX, Active Directory, Bing, Internet Explorer, MSDN, SharePoint, Silverlight, SQL Server, Visual Basic, Visual Studio, Windows, Microsoft Intune, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Revision History

Release Date	Changes
April 26, 2013	Original release of this guide.
May 9, 2013	Minor updates for additional clarity.
June 5, 2013	Minor updates for additional clarity.
October 3, 2013	Minor updates.
January 8, 2015	Various updates for version 3.1
December 17, 2018	Minor update – corrected a link
August 5, 2020	Minor updates and enhancements

Contents

Deployment Guide for System Center Service Manager Exchange Connector	4
Install Exchange Connector	4
Prerequisites	4
Prerequisites to setup OAuth	5
Installation Steps.....	6
Configure the Exchange Connector	7
Configure the Exchange Connector for OAuth	14
Other Configuration options	19
Office 365 Configuration	19
Recipient Impersonation	20
Selecting Work Item Templates.....	20
Allow Service Manager to add external users	21
Test the Connector	21
Creating Work Items.....	21
Updating Work Items.....	22
Updating Incidents	22
Updating Service Requests	23
Updating Problems	23
Updating Change Requests.....	23
Updating Activities	24
Updating Review Activities	24
Updating Manual Activities	24
End to end solution using Notifications	24
Configuring Email Templates	25
Troubleshooting the Connector.....	26
Known Issues	33

Deployment Guide for System Center Service Manager Exchange Connector

System Center Service Manager Exchange Connector connects Service Manager to Exchange Server to process incoming email messages that are related to work items. After you configure Exchange Connector to monitor Exchange mailboxes, it can be used to create and update work items that are based on templates that are specified by a Service Manager administrator.

Administrators can specify special keywords to search for in the incoming email messages, so that Exchange Connector can approve or reject review activities, or enable activity implementers to mark activities that are assigned to them as completed.

The Exchange Connector 4.0 release is compatible with and requires System Center 2016 Service Manager or later versions. It is fully supported by Microsoft.

This release contains bug fixes, and performance improvements as detailed below:

- Whenever a manual activity task gets completed, Exchange Connector now updates the closing time to the current time of closing, which was not set earlier.
With this fix, when a customer sends a request to close an incident which is already closed, the incident remains closed, which was not the case earlier.
- This release contains all the fixes in the previous release
- Adds support to OAuth 2.0 based authentication for EWS to connect to Exchange Online.

Install Exchange Connector

The following sections explain the prerequisites, installation steps, and upgrade steps for Exchange Connector 4.0.

Prerequisites

To set up the Exchange Connector, the following files are required. Download them from [here](#).

- Exchange Web Services Managed API Client DLL (Microsoft.Exchange.WebServices.dll),
- Microsoft.SystemCenter.ExchangeConnector.dll,
- Microsoft.Identity.Client.dll,
- Microsoft.SystemCenter.ExchangeConnector.resources.dll and
- ServiceManager.ExchangeConnector.mpb.

Prerequisites to setup OAuth

We use the OAuth authentication service, provided by Azure Active Directory to enable EWS Managed API applications and access Exchange Online in Office 365. As per Industry-standard protocols OAuth 2.0 and OpenID Connect, only Office 365 AAD accounts are the supported audience for this scenario.

See the following articles for more information.

- [Scenarios and supported authentication flows](#)
- [Authentication library](#)

To use OAuth with Exchange Connector application, you need to register an application with Azure Active Directory. Use the following steps to register an application:

1. Open a browser and navigate to [Azure Active Directory admin center](#), and login using **Azure Admin account**.
2. Select **Azure Active Directory** in the left-hand navigation, and then select **App registrations** under **Manage**.
3. Select **New registration**. On the **Register an application** page, set the values as follows.
 - a. Set **Name** to a friendly name for your app.
 - b. Set **Supported account types** to the choice that is appropriate for your scenario.
 - c. For **Redirect URI**, select the drop-down to **Public client (mobile & desktop)** and set the value to urn:ietf:wg:oauth:2.0:oob.
4. Choose **Register**. On the next page, copy the value of the **Application (client) ID** and save it, you will need it later.
5. Select **API permissions** in the left-hand navigation under **Manage**.
6. Select **Add a permission**. On the **Request API permissions** page, select **Exchange** under **Supported legacy APIs**.
7. To use Delegated permissions, select **Delegated permissions** and then select **EWS.AccessAsUser.All** under **EWS**. Click **Add permissions**.
8. Select **Grant admin consent for org** and accept the consent dialog.
9. Lastly, keep a copy of Application ID and Tenant ID; this data will be used while setting up Exchange Connector with Office 365 Mailbox.
10. On the left panel, click **Authentication**.
11. Make sure **Default client type** is set to **Yes**.



Default client type ⓘ

Treat application as a public client.
Required for the use of the following flows where a redirect URI is not used:

Yes No

12. Click on **Save**

For more information, see [How to authenticate an application by using OAuth](#).

Installation Steps

Below steps are also applicable for upgrade from the Exchange Connector 3.1. To install from the, `System_Center_Service_Manager_Connector_4.0_for_Exchange.exe`, use the following steps:

Note: During installation, are prompted to extract the installation files to a default folder. The default location is “***InstallationDrive:\System Center Service Manager Connector 4.0 for Exchange***”.

Use the

1. Run the Setup file.
2. After you have installed the Exchange Connector, copy the DLL files, `Microsoft.SystemCenter.ExchangeConnector.dll`, `Microsoft.Identity.Client.dll` and `Microsoft.SystemCenter.ExchangeConnector.resources.dll`, to your Service Manager installation folder.
Example: `<InstallationDrive>Program Files\Microsoft System Center\Service Manager`
3. Import the `ServiceManager.ExchangeConnector.mpb` to the management server. This imports the following two management packs:
 - `Microsoft.SystemCenter.ExchangeConnector`
 - `Microsoft.SystemCenter.ServiceManager.ChangeRequestActionLog`
4. Copy `Microsoft.Exchange.WebServices.dll` to the Service Manager management server from the Service Manager installation folder.
5. If you need to use account impersonation for the Run As account that Exchange Connector will use, run the following command in Windows PowerShell.

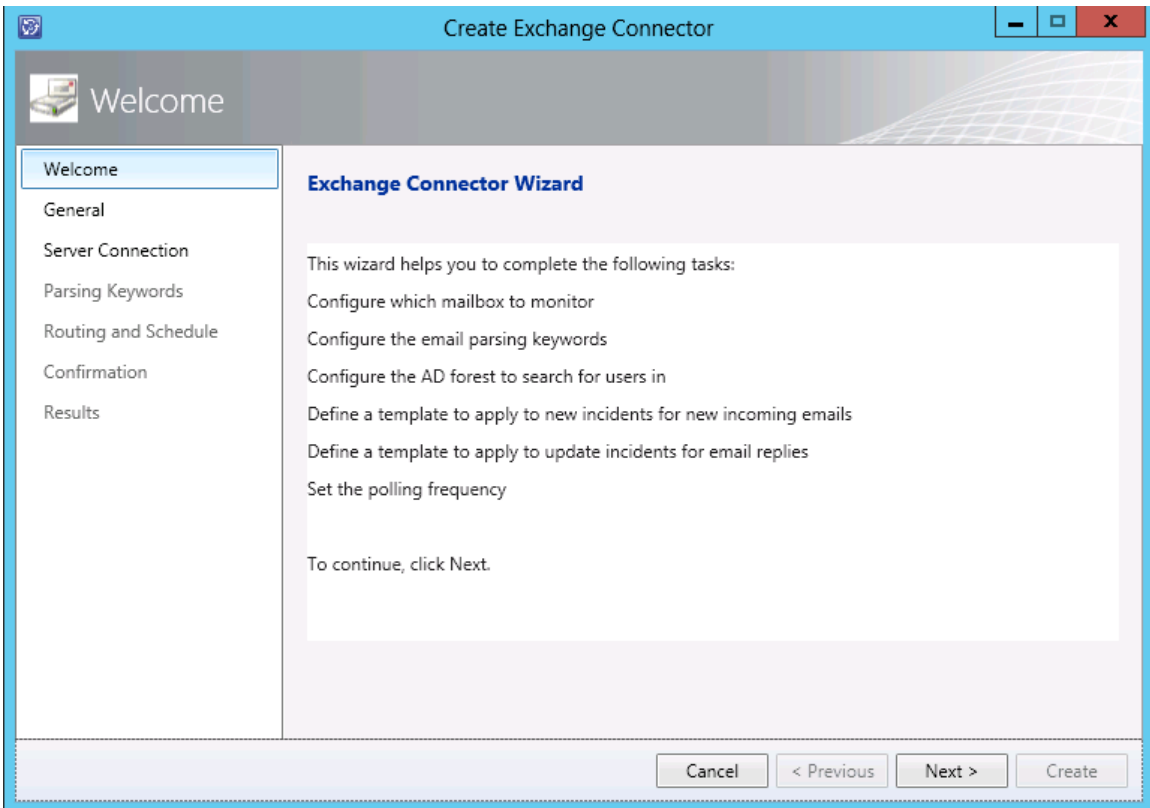
```
New-ManagementRoleAssignment -Name:AdminImpersonateAll -  
Role:ApplicationImpersonation -User SCSMWorkflow
```
6. Create and configure a server authentication certificate for Exchange Server by using the following steps:
 - a. If your Service Manager management server does not have a trusted relationship with the Exchange Server, open Certificate Services and create a duplicate copy of the Web Server Certificate Template. Ensure that **Private Key Export** and **Publish**

- in AD** are selected, and then add **Read and Enroll** permission to Authenticated Users.
- b. In **Certificate Services**, navigate to **Certificate Template** and right-click **Certificate Templates**. Click **New**, and then click **Certificate Template to Issue**. Select the template that you created in the previous step.
 - c. In Exchange Server, open the Microsoft Management Console and add the **Certificates** snap-in for the local computer. Right-click the **Personal** logical store, and then hover over **All Tasks**.
 - d. Select **Request for New certificate** and in the **Certificate Enrollment** wizard, select **Active Directory Enrollment Policy** and select the template that you created previously. When you select the certificate, you can click **More Information** to type the Exchange Server's FQDN name as the common name in the **Subject** tab. You can also type the FQDN name as the **Friendly Name** in the **General** tab.

Configure the Exchange Connector

Use the following procedure:

1. Open the Service Manager console and navigate to **Administration, Connectors**.
2. Click **Create Connector**, and then, in the Task pane, click **Exchange**.
3. In the **Create Exchange Connector** wizard, perform the following steps:
 - a. On the Welcome page, click **Next**.



- b. On the **General** page, provide a name and description for the connector, and type the name of the Active Directory forest that is used by users who send email to Service Manager. If there is more than one forest, separate them with semi-colons. Then, select from the following choices and click **Next**:
- If you want Exchange Connector to attach the email message that is received to the work item that is created or updated, select **Attach each email as a .eml file attachment to the work item**.
 - If you want to allow Exchange Connector to process email and create work items from unknown users, do not select **Only process emails from users in the CMDB**.



Note

This option increases potential risks to security

Each time that an email message is received from a sender that was previously unknown, Exchange Connector creates a new user in the Service Manager database and associates the user with the work item. This option defines actions to take or not take when an email is received, such as creating or updating a work item. However, it doesn't change how emails are read. For example, email is still marked as read and deleted, if you select the option **Move email to Deleted Items after processing**.

- iii. If you want email to be deleted from the user's Exchange or Office 365 account, select **Move email to Deleted Items after processing**. This choice does not permanently delete the items, but they will be subject to your organization's Exchange policies that automatically delete items in the Deleted Items folder.
- iv. If you want to add the text content of email messages to the new or updated work item's action log, select **Append the full body of the email message (up to 4,000 characters) to the action log**.
- v. Select **Enable this connector** to enable the connector.

The screenshot shows the 'Create Exchange Connector' wizard in the 'General Settings' step. The window title is 'Create Exchange Connector'. On the left, a navigation pane lists: Welcome, General (selected), Server Connection, Parsing Keywords, Routing and Schedule, Confirmation, and Results. The main area is titled 'General Settings' and contains the following fields and options:

- Name:** Exchange Connector
- Description:** (Empty text box)
- Enter one or more Active Directory FORESTS (not DOMAINS) to search for users in:** contoso.com
Example: contoso.com;corp.contoso.com;europe.contoso.com
- Attach each email as a .eml file attachment to the work item
- Only process emails from users in CMD8
- Move email to Deleted Items after processing
- Append the full body of the email message (up to 4,000 characters) to the action log
- Enable this connector

At the bottom right, there are four buttons: Cancel, < Previous, Next >, and Create.

- c. On the Server Connection page, provide the following information and make the following choices, and then click **Next**.
 - i. If you want to automatically discover the server URL of the monitored email account, select **Use autodiscover**. Learn more about the AutoDiscover service at [Configure Exchange Services for the Autodiscover Service](#).

 **Note**

If you want to manually specify the server URL of the monitored email account instead, clear this option and type the URL in the **Exchange Server URL** field.

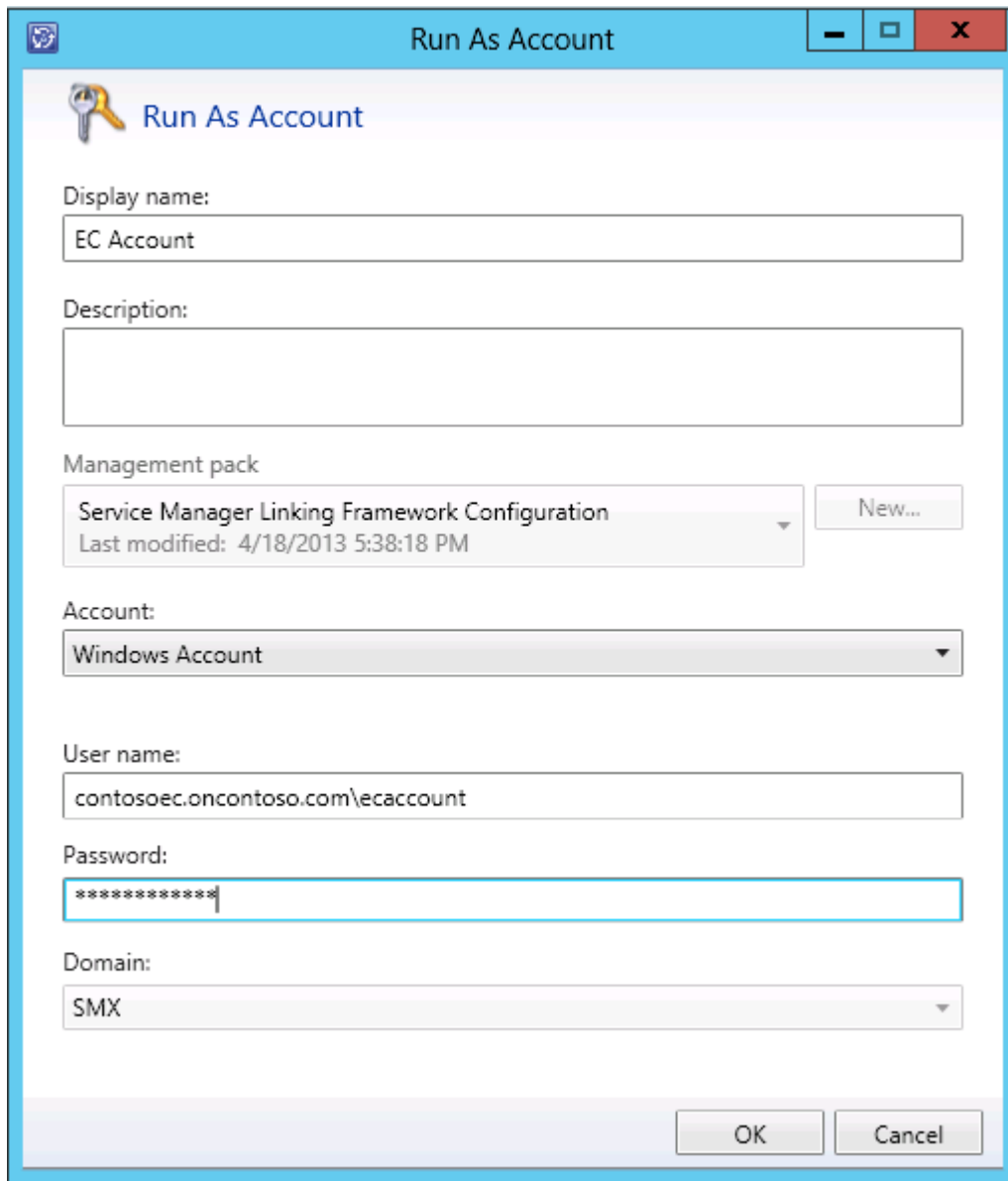
- ii. By default, the **Validate only Office 365 autodiscover redirections** option is enabled and it allows only redirections to `https://Autodiscover-s.outlook.com/Autodiscover/Autodiscover.xml`. If redirections between other domains is required, clear the item or specify the Exchange Server URL manually.
- iii. In the **Exchange Server URL** box, type the URL of the Exchange Server if you do not use AutoDiscover.
- iv. If you want Exchange Connector to impersonate a specific user, select **Use Impersonation**. For more information about impersonation, see the Recipient Impersonation section in this document.
- v. For the Run As account, click **New**.

The screenshot shows the 'Create Exchange Connector' dialog box with the 'Server Connection' tab selected. The 'Server Settings' section includes the following options and fields:

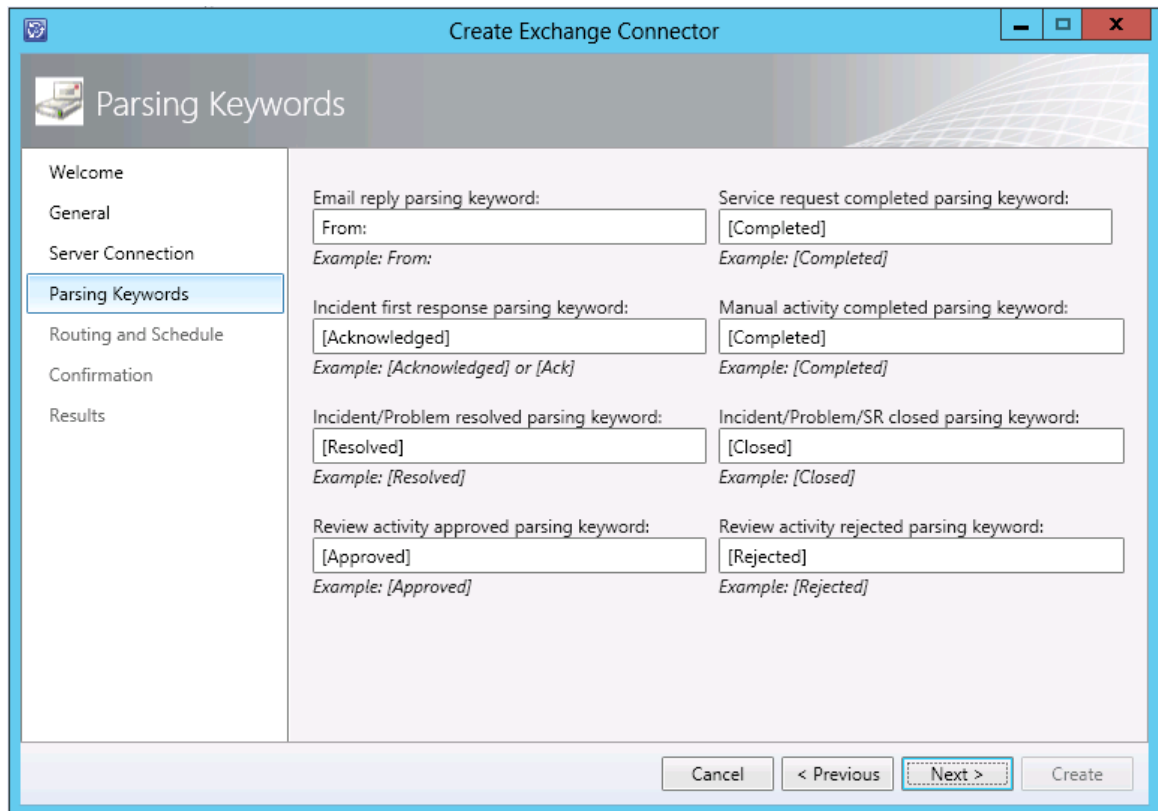
- Use autodiscover
- Validate only Office 365 autodiscover redirections
- Exchange Server URL: [Text Box]
Example: https://pod12345.outlook.com/EWS/Exchange.asmx
- Use impersonation
- Impersonation e-mail address: [Text Box]
Example: helpdesk@contoso.com
- Run As account: [Dropdown Menu] EC Account [New...]
- [Test Connection]

At the bottom of the dialog, there are buttons for 'Cancel', '< Previous', 'Next >', and 'Create'.

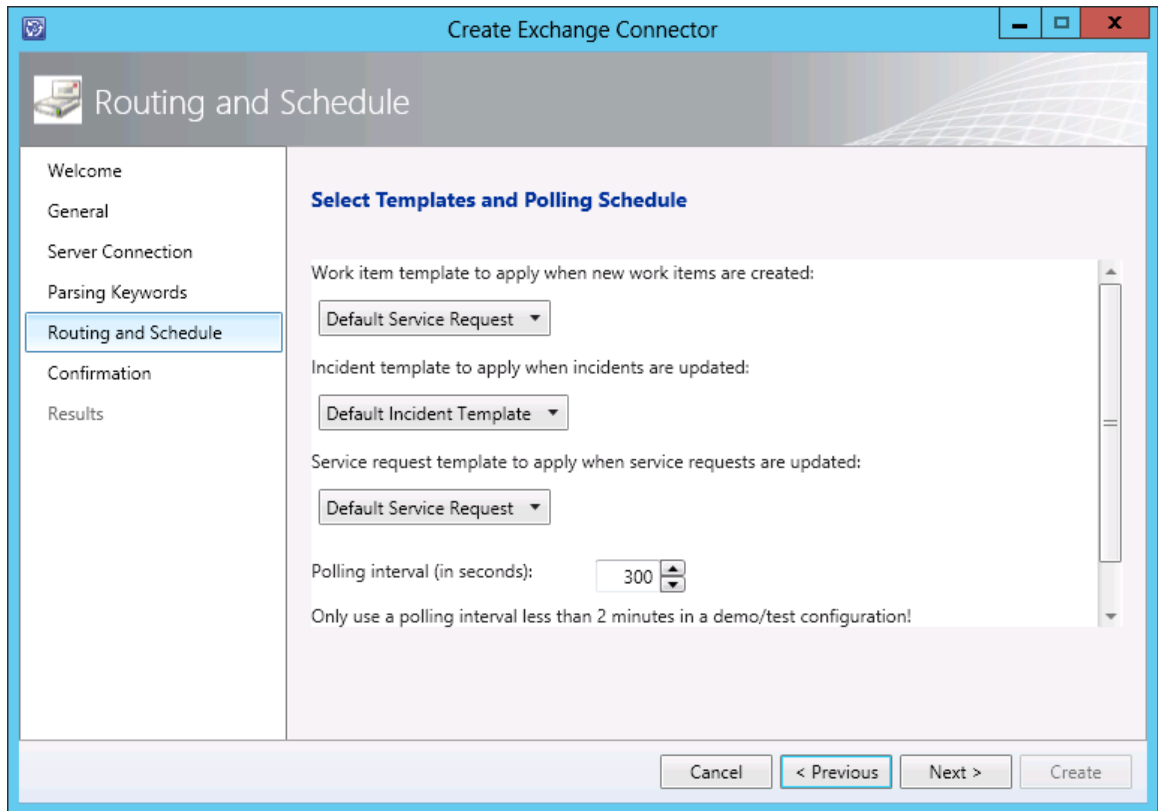
- d. In the **Run As Account** dialog box, enter the account credentials. The workflow account that you use must have an Office 365 or Exchange 2010 mailbox. Ensure that the email address of the account that you enter is in down-level logon name format (for example, **DOMAINUserName**).



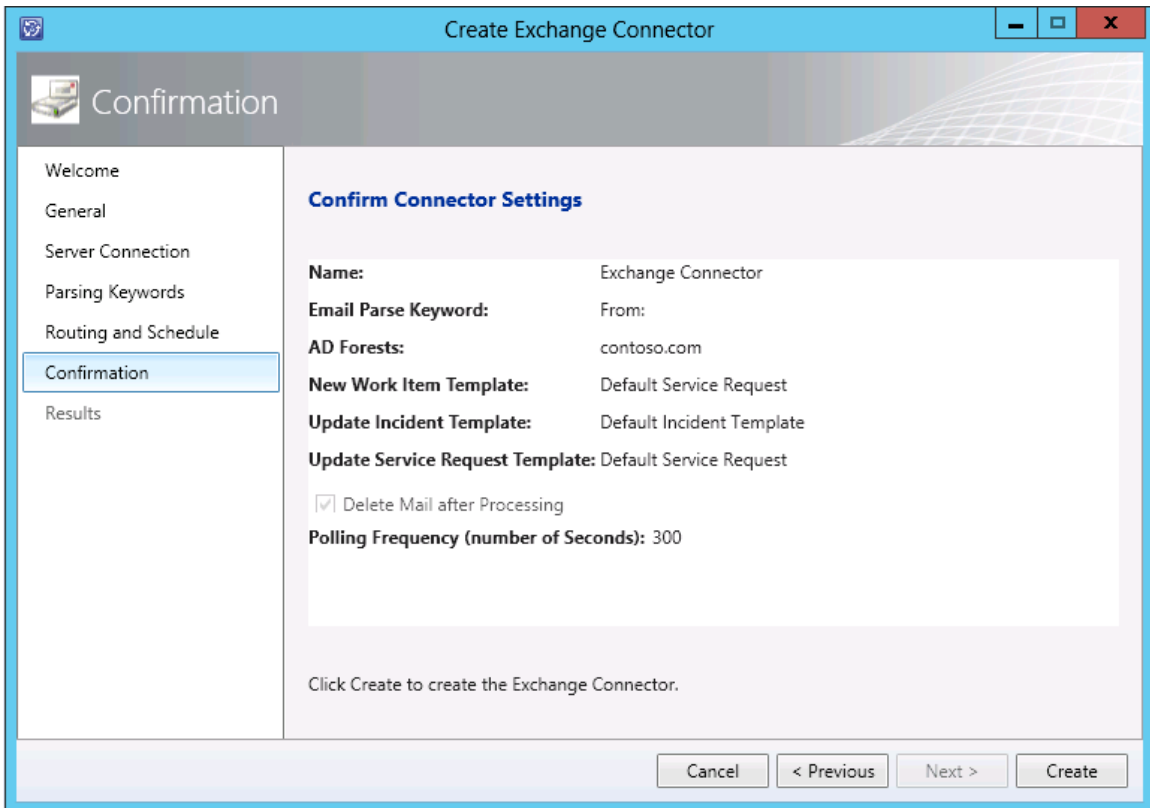
- e. On the **Parsing Keywords** page, choose various keywords to look for to perform various status and value changes such as **[Resolved]**, **[Closed]**, and so on. You can use the choice of words and phrases you like, but ensure that you choose a string value that would not normally occur in regular email conversation by enclosing the text in square brackets.



- f. On the **Routing and Schedule** page, choose the templates to apply when work items are created or updated, specify the polling interval that Service Manager should use to check for new messages, and then click **Next**.



- g. On the **Confirmation** page, review the information and then click **Create**.



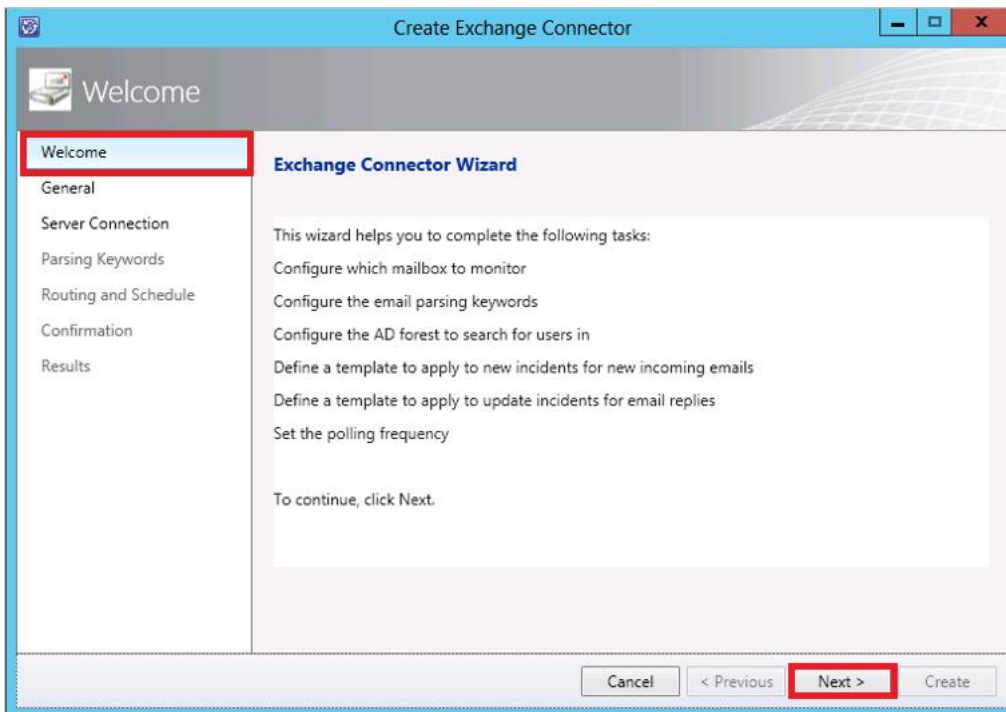
- h. On the **Results** page, click **Close**.

Configure the Exchange Connector for OAuth

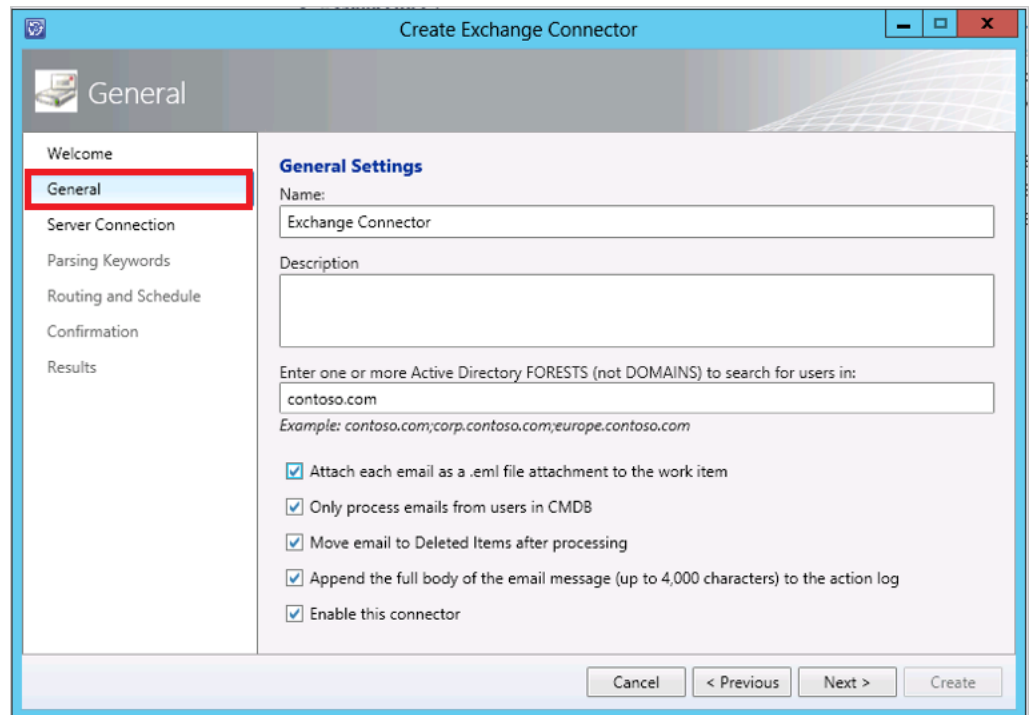
Use the following steps:

1. Open the Service Manager console and navigate to **Administration, Connectors**.
2. Click **Create Connector**, and then, in the Task pane, click **Exchange**.
3. In the **Create Exchange Connector** wizard, do the following steps:

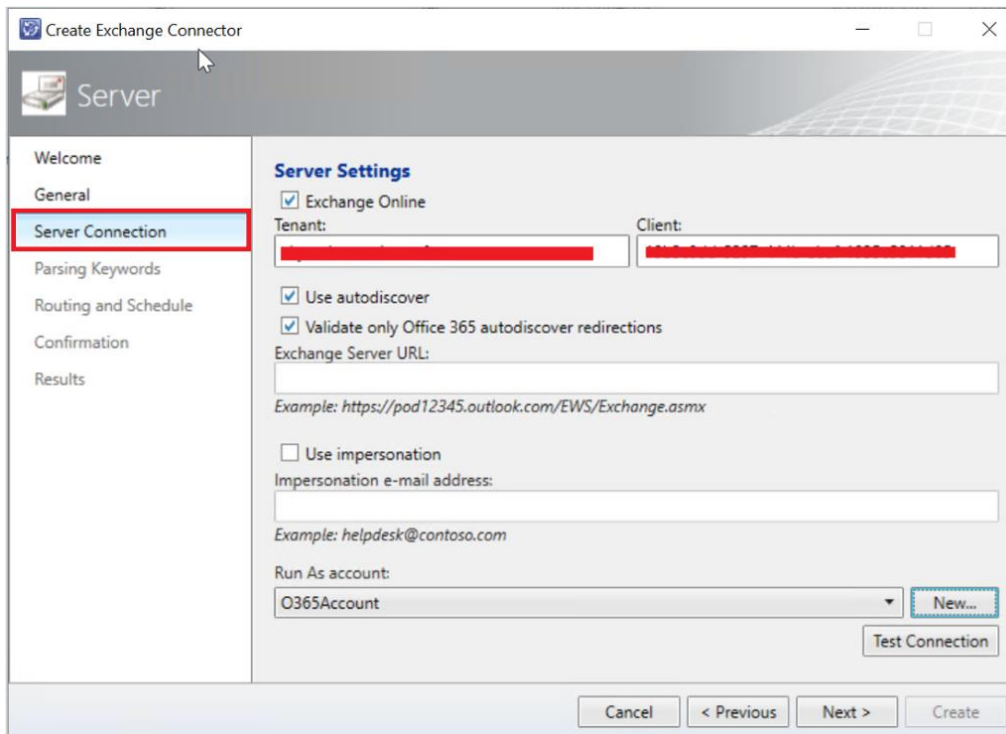
On the Welcome page, click **Next**.



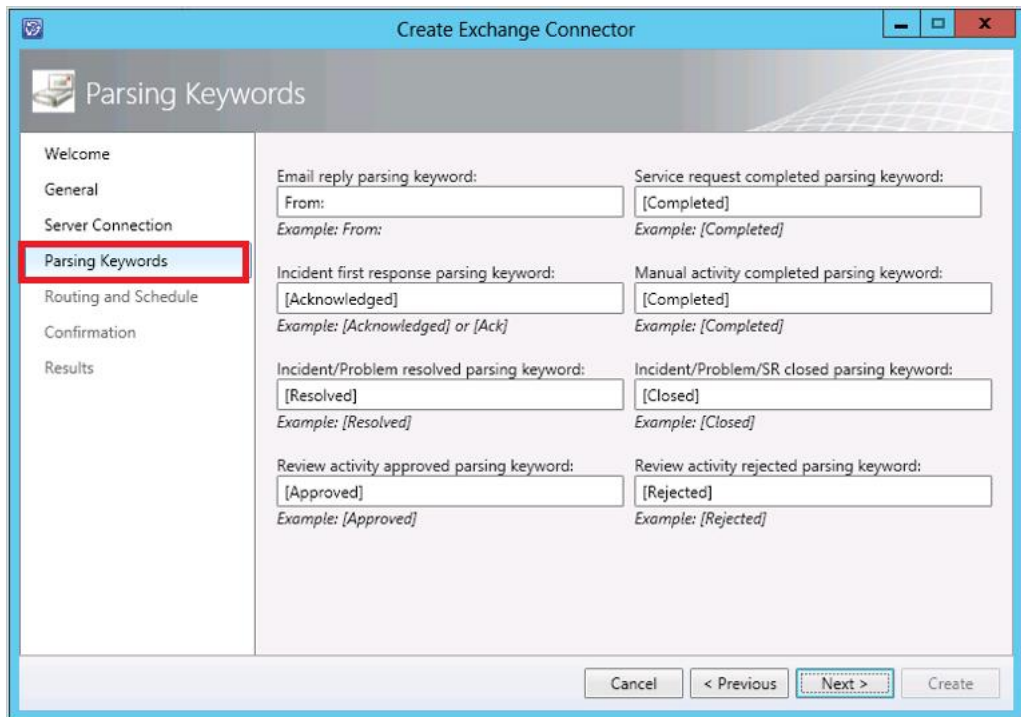
- a. On the **General** page, provide a name and description for the Connector, and type the name of the Active Directory forest that is used by users, who send email to Service Manager. If there is more than one forest, separate them with semi-colons. Then, select from the following choices and click **Next**:
 - i. If you want Exchange Connector to attach the email message that is received to the work item that is created or updated, select **Attach each email as a .eml file attachment to the work item**.
 - ii. If you want to allow Exchange Connector to process email and create work items from unknown users, do not select **Only process emails from users in the CMDB**.
 - iii. If you want email to be deleted from the user's Exchange or Office 365 account, select **Move email to Deleted Items after processing**. This choice does not permanently delete the items, but they will be subject to your organization's Exchange policies that automatically delete items in the Deleted Items folder.
 - iv. If you want to add the text content of email messages to the new or updated work item's action log, select **Append the full body of the email message (up to 4,000 characters) to the action log**.
 - v. Select Enable this connector to enable the connector.



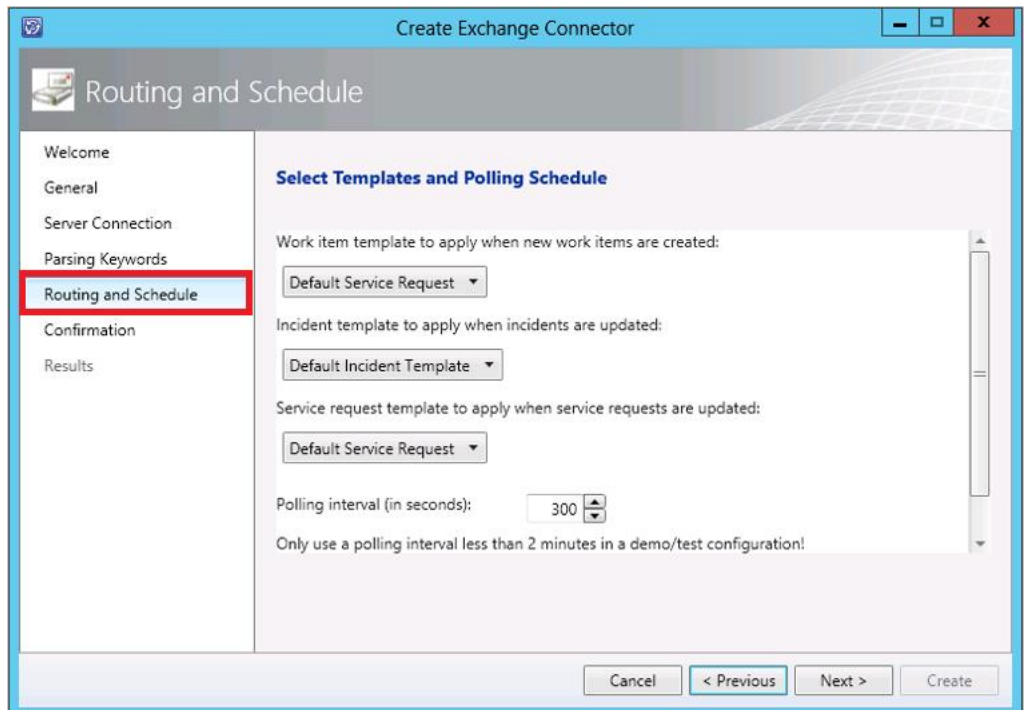
- b. On the **Server Connection** page, provide the following information and make the following choices, and then click **Next**.
- i. Select **Exchange Online**.
 - ii. In the **Tenant and Client** box, enter the Tenant ID and Application Client ID
 - iii. If you want to automatically discover the server URL of the monitored email account, select **Use autodiscover**.
Note: If you want to manually specify the server URL of the monitored email account instead, follow the steps in the section [Office 365 Configuration without Autodiscover](#).
 - iv. By default, the **Validate only Office 365 autodiscover redirections** option is enabled and it allows only redirections to <https://Autodiscover-s.outlook.com/Autodiscover/Autodiscover.xml>. If redirections between other domains is required, clear the item, or specify the Exchange Server URL manually.
 - v. If you want Exchange Connector to impersonate a specific user, select **Use Impersonation**. For more information about impersonation, see the Recipient Impersonation section earlier in this document.
 - vi. For the **Run As account**, click **New**.



- vii. In the **Run As Account** dialog box, enter the account credentials. The workflow account that you use must have an Office 365 or Exchange 2010 mailbox. Ensure email address is entered in Username box.
- c. On the **Parsing Keywords** page, choose various keywords to look for to perform various status and value changes such as **[Resolved]**, **[Closed]**, and so on. You can use the keywords and phrases of your choice, but ensure that you choose a string value that would not normally occur in regular email conversation by enclosing the text in square brackets.



- d. On the **Routing and Schedule** page, choose the templates to apply when work items are created or updated, specify the polling interval that Service Manager should use to check for new messages, and then click **Next**.



- e. On the **Confirmation** page, review the information and then click **Create**.
- f. On the **Results** page, click **Close**.

Other Configuration options

The following sections describe other configuration options that you can use to enhance the Exchange Connector's functionality.

Office 365 Configuration

If you're using an Office 365 account with the Exchange Connector, then you need to configure it differently than an Exchange Server account. During configuration, do not select Autodiscover—instead, use the standard Office365 Exchange Server URL, as shown in the following image.

Server Settings

Use autodiscover

Validate only Office 365 autodiscover redirections

Exchange Server URL:

<https://outlook.office365.com/EWS/Exchange.asmx>

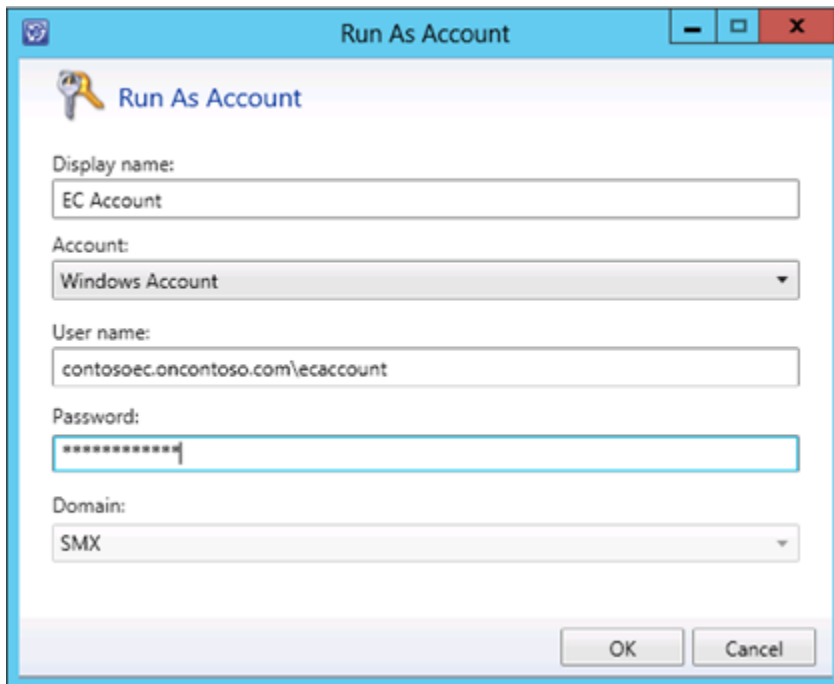
Example: <https://pod12345.outlook.com/EWS/Exchange.asmx>

Use impersonation

Impersonation e-mail address:

Example: helpdesk@contoso.com

For the Run As account, specify the Office 365 address. The domain name is not relevant.



1. Click **OK**. Service Manager displays a warning message that you can ignore.

Recipient Impersonation

Unless you configure Exchange Connector to allow impersonation for other accounts, Exchange Connector can access only the mailbox of the Run As account that is specified in the Create Exchange Connector wizard. If you want to have multiple Exchange Connector instances that monitor different mailboxes, you must configure Exchange Connector to allow the Run As account to impersonate the credentials of the other mailbox recipients.



Note

If you configure Exchange Connector to monitor a mailbox other than the Workflow Run As account's mailbox, ensure that you select **Use impersonation** on the Server Connection page of the Create Exchange Connector wizard.

Selecting Work Item Templates

The template lists are populated with only those templates that are targeted at the Incident (advanced) type projection and Service Request (advanced), or directly at the Incident/Service Request class. If you use the Service Manager console to create templates, they are targeted at the Incident (advanced) or Service Request (advanced) type projection for you, so there is nothing else that you need to do.

Allow Service Manager to add external users

Exchange Connector 4.0 disables automatic addition of email addresses to the Service Manager database (CMDB) from the To or CC lines of an email message. This ensures that external users cannot access Service Manager.

To disable this, you can modify the registry by navigating to the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System Center Service Manager Exchange Connector** node and selecting the **AllowAdditionOfNonSMUsers** key and then setting to value to 1.

Test the Connector

To test the Exchange Connector, send an email message to the Exchange Connector email address. It should be converted into a new work item and the specified template should be applied. Send another email message to the same address and put the newly created work item's ID in the subject line.



Note

The work item ID must be enclosed in square brackets. For example, **[IR1234]** works, but **IR1234** does not work.

The work item should be updated. Test other scenarios by sending email messages with various work item IDs in the subject, enclosed in square brackets, and using different keywords such as **[Resolved]**, **[Approved]**, and so on, depending on what type of work item you are trying to update and what keywords you configured the connector to look for.

Creating Work Items

When an email is sent to an Exchange mailbox that is being monitored by Exchange Connector, and no work item ID is present in the subject, Exchange Connector processes the incoming email and creates a new work item. The email subject becomes the work item title. The email body becomes the work item description. Any attachments to the message are added to the work item as related file attachments. The sender becomes the Affected User. Any To or CC recipients besides the mailbox that Exchange Connector is monitoring are added as Related Items, not as Affected Users. The Created By User is set to the user corresponding to the Run As Account that was specified in the Create Exchange Connector wizard.

When the new work item is created, a configurable template can be applied to automatically route and escalate the work item by assigning it to the appropriate person and support group, and assigning it the appropriate urgency, impact, and so on. The type of work item that is created is determined by the target class or type projection that the selected template was created for. In other words, if you select an incident template an incident work item is created; if you select a service request template, a service request work item is created.

Some special logic applies if the Exchange Connector is creating an incident work item. If you select an incident template that does not specify the impact or urgency, those properties are set

to Low. If you do not specify the source in the template, the incident source is set to E-mail. If you do not specify the status, the incident is set to Active.

Exchange Connector includes the Change Request Action log management pack, and the management pack is installed as part of the connector. This management pack is used by the connector to update the action log field with the contents of the most recent email to the action log field.

Updating Work Items

The Service Manager Exchange Connector currently supports the following scenarios for updating work items:

- Updating Incidents
- Updating Service Requests
- Updating Problems
- Updating Change Requests
- Updating Manual Activities and Review Activities

Updating Incidents

When Exchange Connector processes an email message about an existing incident, and the message has the incident ID in the subject line, for example **Sample Incident [IR1234]**, the connector appends the email message to the action log of the incident that is identified by the ID in the subject line. When the incident is updated, a configurable template can be applied to the incident to classify or route it appropriately. Any file attachments in the email message are also added to the incident. Any To or CC recipients besides the mailbox that Exchange Connector is monitoring are added (if they are not already present) as Related Items, not as Affected Users. If the keyword for acknowledging the incident, for example **[Acknowledged]**, is present in the body of the email message, the **FirstResponse** date property is set to **Now** if it is not already set.

When an email message with an incident ID in the subject also contains the configurable keyword for resolving, for example **[Resolved]**, or closing **[Closed]**, the connector does the following:

1. Changes the status of the incident accordingly, updates the action log, and attaches any files.
2. Adds the sending user as the resolving or closing user.
3. Adds the content of the most recent email message to the resolution description field when the **[Resolved]** keyword is sent.
4. Resolves and closes the incident (in separate transactions) if both the **[Resolved]** and the **[Closed]** keywords are present. First, the resolution is logged in the database immediately, followed by the close update. This ensures that any workflows that are triggered by a change to the resolved status are triggered. Additionally, if the **[Closed]** keyword is present and the incident is not currently in the resolved state, the incident is first resolved and then closed to ensure that all resolution workflows are triggered.

Updating Service Requests

When an email message is processed by Exchange Connector for an existing service request that contains the service request ID in the subject, for example **Sample Service Request [SR1234]**, the connector appends the email message to the action log of the service request that is identified in the subject by the ID. When the service request is updated, a configurable template can be applied to the service request to classify or route it appropriately. Any file attachments in the message are also added to the service request. Any To or CC recipients besides the mailbox that Exchange Connector is monitoring are added (if they are not already present) as Related Items, not as Affected Users.

There are two service request update processes:

- There are child activities, which must be completed in a sequence. While the activities are being completed, the service request has a status of **In Progress**. When all of the activities are complete, the system automatically marks the service request status as **Completed**.
- There are no child activities. In this case, the service request status is **Submitted**. When the service request is fulfilled, the status changes to **Completed**.

If the mail body contains the service request completed keyword, for example **[Completed]**, the behavior differs, depending on the service request lifecycle. If the service request status is **In Progress**, for example following the first update process in the preceding list, Exchange Connector does nothing because the child activities could have various statuses and the service request may not actually be complete. In that case, Service Manager logs an error message to the event log. In the second case, where there are no child activities and the service request status is **Submitted**, the connector changes the status to **Completed**. If the mail body contains the keyword **[Closed]**, the service request status is set to closed.

Updating Problems

When an email message is processed by Exchange Connector for an existing problem record that contains the problem record ID in the subject, for example **Sample Problem [PR1234]**, the connector appends the email message to the action log of the problem that is identified in the subject by the ID. Any file attachments in the email message are also added to the problem record. Any To or CC recipients besides the mailbox that Exchange Connector is monitoring are added (if they are not already present) as Related Items, not as Affected Users. If the incoming email message contains the **[Resolved]** or **[Closed]** keywords, Exchange Connector updates the status of the problem to the specified status.

Updating Change Requests

When an email message is sent with a change request work item ID in the subject, the connector updates the action log field and adds the content of the most recent email message. Any email attachments are added as file attachments to the change request. Any To or CC recipients besides the mailbox that Exchange Connector is monitoring are added (if they are not already present) as Related Items, not as Affected Users.

Updating Activities

Exchange Connector can update review activities and manual activities.

Updating Review Activities

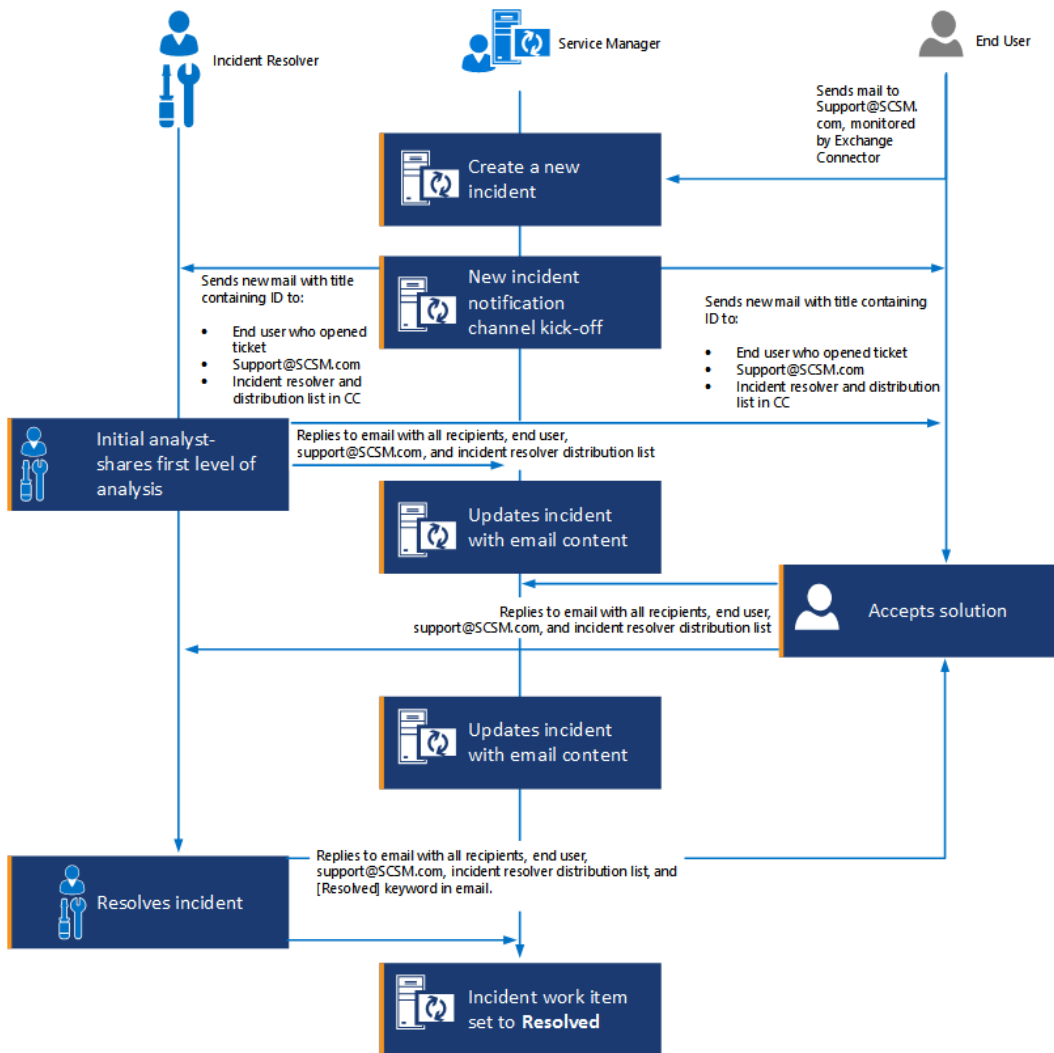
If an email message is sent with a review activity ID in the subject, and the most recent message body contains the configurable keyword for approving, for example **[Approved]**, or rejecting, **[Rejected]**, the connector changes the vote status for the sending user in the review activity, if the sender is a reviewer. This approach cannot be used to change the vote status of a use group. If both the approved and rejected keywords are sent, the connector changes the vote to **Rejected** to be safe. The sender can change the vote status by sending another email message. Any email attachments are added as file attachments to the review activity. If the review activity does not have a status of **In Progress**, Exchange Connector does not update the vote, but logs an error event in the event log. Any To or CC recipients besides the mailbox that Exchange Connector is monitoring are added (if they are not already present) as Related Items, not as Affected Users.

Updating Manual Activities

If an email message is sent with a manual activity ID in the subject, the connector appends the contents of the latest message body (up to 4,000 characters) to the **Notes** field. If the configurable keyword for completion of the activity is present, for example **[Completed]**, the connector changes the status of the activity to **Completed**. Any email attachments are added as file attachments to the review activity. Any To or CC recipients besides the mailbox that Exchange Connector is monitoring are added (if they are not already present) as Related Items, not as Affected Users.

End to end solution using Notifications

The Exchange Connector provides easy way to create or update work items in Service Manager, but it has limitations— it can only read emails and no information is provided to the end user about the final result of an update. To overcome this, you can configure Exchange Connector with using notifications in Service Manager to accomplish work items management using only emails. So there is no need to access Service Manager through the Self-Service Portal or the Service Manager console. The following diagram shows the simple end-to-end management process for incidents.



Configuring Email Templates

If you plan to configure email templates for use with Exchange Connector, you can use the SendEmail solution. For more information about the SendMail solution, see [System Center Service Manager – Exchange Connector](#), which is part of a previous release of Exchange Connector.

Ensure that the following information is true before you deploy the connector.

Each email message that is sent out from Service Manager must contain the work item ID enclosed in square brackets in the subject line, so that when people reply, the work item ID is in the subject and can be processed by the connector. Remember that if the work item ID is not present in the subject, the connector processes the message as a new incident. To avoid this problem, insert the Work Item ID property in all of the notification templates that are used to send email about work items.

Review the following blog posts for ideas about how to configure notification templates, subscriptions, and workflows for various scenarios:

- [Sending Notifications to Reviewers When a Review Activity Becomes Active](#) The approach for manual activities is similar to the one at this link.
- [Custom notification workflow on incident assignment or re-assignment](#)
- [Custom Notification workflow on activity assignment or reassignment](#)

Other useful blog posts about how to configure notifications include the following:

- [Inserting links to Review/Manual Activities in notifications](#)
- [Creating Notification Templates in System Center Service Manager](#)
- [Using And/Or Criteria in Workflow and Notification Subscriptions](#)
- [Automatically Notifying Groups of Users](#)
- [Workflow/Notification Subscription NotEqual Criteria Across Pre/Post Condition](#)
- [Sending Notifications to Users in Different Languages](#)

Troubleshooting the Connector

Each time Exchange Connector runs, it logs events into the Operations Manager event log on the Service Manager management server on which the workflows run. By default, this is the first management server installed in a management group. The source appears as **Exchange Connector**. If there is a crash in the connector, the error is handled and the error message is logged in an error event from the **Health Service Modules** source.

By default, Exchange Connector logs only error events into the event log. There are two registry values that you can configure to log additional details. To do that, create the following registry key if it does not already exist:




**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\System Center Service Manager
Exchange Connector**

Then, create the following string values:

EnableEWSTracing

LoggingLevel

The following image is an example.

Name	Type	Data
 (Default)	REG_SZ	(value not set)
 EnableEWSTracing	REG_SZ	1
 LoggingLevel	REG_SZ	7

You can set the LoggingLevel value to any number from 1 to 7. The higher the number, the more detailed and verbose the logging is. If the value is set to 0 or the value does not exist, then only error events are created in the event log.

If **EnableEWSTracing** value is set to 1, the Exchange web service tracing events are logged to the event log. If the **EnableEWSTracing** value is not created or if it is set to 0, the events for the

Exchange web service tracing are not recorded in the event log. If **EnableEWSTracing** is set to 1, the first set of information events shows the details of the connector operations as the connector tries to determine which Exchange server to communicate with, based on the Exchange Auto Discover Service configuration in AD and DNS.

The following log entries are examples that indicate the system is working properly.

<pre>AutodiscoverConfiguration: <EwsLogEntry EntryKind="AutodiscoverConfiguration" ThreadId="4" Timestamp="1/6/2011 7:33:03 PM">Starting SCP lookup for domainName='fabrikam.com', root path='</EwsLogEntry></pre>
<pre>AutodiscoverConfiguration: <EwsLogEntry EntryKind="AutodiscoverConfiguration" ThreadId="4" Timestamp="1/6/2011 7:33:03 PM">Searching for SCP entries in LDAP://CN=Configuration,DC=fabrikam,DC=com</EwsLogEntry></pre>
<pre>AutodiscoverConfiguration: <EwsLogEntry EntryKind="AutodiscoverConfiguration" ThreadId="4" Timestamp="1/6/2011 7:33:03 PM">Scanning for SCP pointers Domain=fabrikam.com</EwsLogEntry></pre>
<pre>AutodiscoverConfiguration: <EwsLogEntry EntryKind="AutodiscoverConfiguration" ThreadId="4" Timestamp="1/6/2011 7:33:03 PM">No SCP pointers found for 'Domain=fabrikam.com' in configPath='CN=Configuration,DC=fabrikam,DC=com'</EwsLogEntry></pre>
<pre>AutodiscoverConfiguration: <EwsLogEntry EntryKind="AutodiscoverConfiguration" ThreadId="4" Timestamp="1/6/2011 7:33:03 PM">Scanning for SCP urls for the current computer Site=Default-First-Site-Name</EwsLogEntry></pre>
<pre>AutodiscoverConfiguration: <EwsLogEntry EntryKind="AutodiscoverConfiguration" ThreadId="4" Timestamp="1/6/2011 7:33:03 PM">Adding (prio 1) 'https://SMDC.fabrikam.com/Autodiscover/Autodiscover.xml' for the 'Site=Default-First- Site-Name' from 'LDAP://CN=SMDC,CN=Autodiscover,CN=Protocols,CN=SMDC,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=fabrikam,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=fabrikam,DC=com' to the top of the list (exact match)</EwsLogEntry></pre>
<pre>AutodiscoverConfiguration: <EwsLogEntry EntryKind="AutodiscoverConfiguration" ThreadId="4" Timestamp="1/6/2011 7:33:03 PM">Trying to call Autodiscover for administrator@fabrikam.com on https://SMDC.fabrikam.com/Autodiscover/Autodiscover.xml.</EwsLogEntry></pre>
<pre>AutodiscoverRequest: <EwsLogEntry EntryKind="AutodiscoverRequest" ThreadId="4" Timestamp="1/6/2011 7:33:09 PM"></pre>

```
<Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschem/2006">
  <Request>
    <EmailAddress>administrator@fabrikam.com</EmailAddress>
  </Request>
  <AcceptableResponseSchema>http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a</AcceptableResponseSchema>
</Autodiscover>
</EwsLogEntry>
```

```
AutodiscoverResponseHttpHeaders: <EwsLogEntry
EntryKind="AutodiscoverResponseHttpHeaders" ThreadId="4" Timestamp="1/6/2011 7:33:09
PM">200 OK
Persistent-Auth: true
Content-Length: 2272
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Date: Fri, 07 Jan 2011 01:33:09 GMT
Server: Microsoft-IIS/7.5
WWW-Authenticate: Negotiate oRswGaADCgEAoxIEEAEEAABDh+CIwTbjqQAAAAA=
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
</EwsLogEntry>
```

```
AutodiscoverResponse: <EwsLogEntry EntryKind="AutodiscoverResponse" ThreadId="4"
Timestamp="1/6/2011 7:33:09 PM">
  <?xml version="1.0" encoding="utf-8"?>
  <Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
    <Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a"
>
      <User>
        <DisplayName>Administrator</DisplayName>
      </User>
    </Response>
  </Autodiscover>
</EwsLogEntry>
```

```

    <LegacyDN>/o=Fabrikam/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT) /cn=Recipients/cn=Administrator</LegacyDN>

    <DeploymentId>2c28cbbc-6d7b-435d-a60a-e410db5f2901</DeploymentId>

</User>

<Account>

    <AccountType>email</AccountType>

    <Action>settings</Action>

<Protocol>

    <Type>EXCH</Type>

    <Server>SMDC.fabrikam.com</Server>

    <ServerDN>/o=Fabrikam/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT) /cn=Configuration/cn=Servers/cn=SMDC</ServerDN>

    <ServerVersion>7380827F</ServerVersion>

    <MdbDN>/o=Fabrikam/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT) /cn=Configuration/cn=Servers/cn=SMDC/cn=Microsoft Private MDB</MdbDN>

    <AD>SMDC.fabrikam.com</AD>

    <ASUrl>https://smdc.fabrikam.com/EWS/Exchange.asmx</ASUrl>

    <EwsUrl>https://smdc.fabrikam.com/EWS/Exchange.asmx</EwsUrl>

    <EcpUrl>https://smdc.fabrikam.com/ecp</EcpUrl>

    <EcpUrl-um>?p=customize/voicemail.aspx&amp;exsvurl=1</EcpUrl-um>

    <EcpUrl-
aggr>?p=personalsettings/EmailSubscriptions.slab&amp;exsvurl=1</EcpUrl-aggr>

    <EcpUrl-
mt>PersonalSettings/DeliveryReport.aspx?exsvurl=1&amp;IsOWA=&lt;IsOWA&gt;&amp;MsgID=&lt;
;MsgID&gt;&amp;Mbx=&lt;Mbx&gt;&lt;/EcpUrl-mt>

    <EcpUrl-sms>?p=sms/textmessaging.slab&amp;exsvurl=1</EcpUrl-sms>

    <OOFUrl>https://smdc.fabrikam.com/EWS/Exchange.asmx</OOFUrl>

    <UMUrl>https://smdc.fabrikam.com/EWS/UM2007Legacy.asmx</UMUrl>

    <OABUrl>http://smdc.fabrikam.com/OAB/ae7c7c84-b1b9-41c4-9582-
1bf8ee11b009/</OABUrl>

</Protocol>

<Protocol>

    <Type>WEB</Type>

    <Internal>

```

```

    <OWAUrl AuthenticationMethod="Basic,
Fba">https://smdc.fabrikam.com/owa/</OWAUrl>

    <Protocol>

        <Type>EXCH</Type>

        <ASUrl>https://smdc.fabrikam.com/EWS/Exchange.asmx</ASUrl>

    </Protocol>

</Internal>

</Protocol>

</Account>

</Response>

</Autodiscover>

</EwsLogEntry>

```

```

EwsRequest: <EwsLogEntry EntryKind="EwsRequest" ThreadId="4" Timestamp="1/6/2011
7:33:09 PM">

```

```

    <?xml version="1.0" encoding="utf-8"?>

    <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

    <soap:Header>

        <t:RequestServerVersion Version="Exchange2007_SP1" />

        <t:TimeZoneContext>

            <t:TimeZoneDefinition Id="Central Standard Time" />

        </t:TimeZoneContext>

    </soap:Header>

    <soap:Body>

        <m:FindItem Traversal="Shallow">

            <m:ItemShape>

                <t:BaseShape>AllProperties</t:BaseShape>

            </m:ItemShape>

            <m:IndexedPageItemView MaxEntriesReturned="2147483647" Offset="0"
BasePoint="Beginning" />

            <m:Restriction>

                <t:And>

```

```

    <t:IsEqualTo>
      <t:FieldURI FieldURI="message:IsRead" />
      <t:FieldURIOrConstant>
        <t:Constant Value="false" />
      </t:FieldURIOrConstant>
    </t:IsEqualTo>
    <t:IsEqualTo>
      <t:FieldURI FieldURI="item:ItemClass" />
      <t:FieldURIOrConstant>
        <t:Constant Value="IPM.Note" />
      </t:FieldURIOrConstant>
    </t:IsEqualTo>
  </t:And>
</m:Restriction>
<m:ParentFolderIds>
  <t:DistinguishedFolderId Id="inbox" />
</m:ParentFolderIds>
</m:FindItem>
</soap:Body>
</soap:Envelope>
</EwsLogEntry>
EwsResponseHttpHeaders: <EwsLogEntry EntryKind="EwsResponseHttpHeaders" ThreadId="4"
Timestamp="1/6/2011 7:33:09 PM">200 OK
Transfer-Encoding: chunked
Content-Encoding: gzip
Vary: Accept-Encoding
X-EwsPerformanceData: RpcC=2;RpcL=4;LdapC=0;LdapL=0;
Persistent-Auth: true
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Date: Fri, 07 Jan 2011 01:33:09 GMT
Server: Microsoft-IIS/7.5
WWW-Authenticate: Negotiate oRswGaADCgEAoxIEEAEAAAABdh+CIwTbjqQAAAAA=

```

X-AspNet-Version: 2.0.50727

X-Powered-By: ASP.NET

</EwsLogEntry>

EwsResponse: <EwsLogEntry EntryKind="EwsResponse" ThreadId="4" Timestamp="1/6/2011 7:33:09 PM">

<?xml version="1.0" encoding="utf-8"?>

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">

<s:Header>

<h:ServerVersionInfo MajorVersion="14" MinorVersion="0" MajorBuildNumber="722" MinorBuildNumber="0" Version="Exchange2010"

xmlns:h="http://schemas.microsoft.com/exchange/services/2006/types"

xmlns="http://schemas.microsoft.com/exchange/services/2006/types"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/2001/XMLSchema" />

</s:Header>

<s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">

<m:FindItemResponse

xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"

xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types">

<m:ResponseMessages>

<m:FindItemResponseMessage ResponseClass="Success">

<m:ResponseCode>NoError</m:ResponseCode>

<m:RootFolder IndexedPagingOffset="0" TotalItemsInView="0"

IncludesLastItemInRange="true">

<t:Items />

</m:RootFolder>

</m:FindItemResponseMessage>

</m:ResponseMessages>

</m:FindItemResponse>

</s:Body>

</s:Envelope>

</EwsLogEntry>

Your series of events might look somewhat different, but there should not be any errors. If there are errors, it is often due to a configuration problem with the Exchange Auto-Discover service. Learn more about how to configure the Exchange AutoDiscover Service and how to troubleshoot it by using Microsoft Office Outlook at [Configure Exchange Services for the Autodiscover Service](#). Ensure that you are logged into the Service Manager management server on which the connector runs and that you are logged in as the Workflow Run As Account user to be tested.

Known Issues

Description: The Exchange Connector does not filter junk or other emails which should be ignored. For example, mailerdaemon, Out of Office messages, or other spam emails.

Workaround: The best solution is to use Outlook rules to move or delete these mails. Rules need to be configured so that they are applied when mail arrives at the Exchange server and when Exchange Server moves or deletes them before the Exchange connector can process them.

For more information about how to configure rules, see:

- [Exchange Server 2010 and Exchange Server 2013](#)
- [Office 365](#)

Description: Exchange Connector is unable to process mail when the Exchange CAS (Client Access Server) uses Windows Network Load balancing.

Workaround: Forward all communication between Exchange Connector and Exchange Server through the CAS Server. Add an entry in the HOSTS file on the Service Management server to resolve the URL to the IP address of one of the CAS servers.

Description: Exchange Connector should not use the workflow account that is used by other connectors.

Workaround: The workflow account that you use must have an Office 365 or Exchange 2010 mailbox. When you enter Run As account information in the **Run As** dialog box, ensure that the email address of the account that you enter is in down-level logon name format (for example, **DOMAINUserName**).

Description: You cannot create change requests, release records, problem records, or other custom-defined work items by using Exchange Connector.

Workaround: None. You can create only incidents and service requests by using Exchange Connector.

Description: Exchange Connector submits any changes in work items to the Service Manager database immediately. If any workflows require that a status value change from Submitted to Completed, the workflow does not run correctly.

Workaround: None.

Description: Exchange Connector does not update release records.

Workaround: None.

Description: The **Run As Account** dialog box that is used by Exchange Connector does not properly display the account that you chose for the connector.

Workaround: None. However, this is a display problem only. Although the wrong account is displayed, the correct account is used by Exchange Connector.

Description: Exchange Connector does not validate user credentials when you specify a Run As account. When you use Test Connection, the credentials that you specified are stored in the Service Manager database. This can result in erroneous account credentials being stored.

Workaround: None. Ensure that you specify valid Run As account credentials.

Description: The **Percentage** value that is displayed in the Connectors view does not accurately show progress for Exchange Connector. The percentage value that is displayed is always 100. However, the **Status** shown is the correct state.

Workaround: None.

Description: Exchange Connector erroneously allows manual activities to change their state directly from Pending to Completed. However, it should require the state to progress from Pending to In Progress to Completed.

Workaround: None. Inform your users that they should update manual activities after they have verified that a manual activity is progressing from the current state to the intended state.

Description: Exchange Connector erroneously allows problem records to be resolved repeatedly. This can have negative consequences for reporting information because the time at which a problem record is resolved might be unreliable.

Workaround: None. You should verify that a problem record is not already resolved before you update it by using Exchange Connector.

Description: Exchange Connector erroneously allows problem records to be updated when they are in a closed state. They can be updated to Resolved.

Workaround: None. You should verify that a problem record is not already resolved before you update it by using Exchange Connector.

Description: When Exchange Connector processes review activities, and the Approve and Reject keywords are both present in an email message, Approve takes precedence.

Workaround: None. However, you should avoid sending email messages that contain both the Approve and Reject keywords.