Oracle® Cloud

Using the Microsoft Office 365 Outlook Adapter with Oracle Integration Generation 2

ORACLE®

Oracle Cloud Using the Microsoft Office 365 Outlook Adapter with Oracle Integration Generation 2,

E85516-19

Contents

Preface

This guide describes how to configure this adapter as a connection in an integration in Oracle Integration.

> **Note:**
>
> The use of this adapter may differ depending on the features you have, or whether your instance was provisioned using Standard or Enterprise edition. These differences are noted throughout this guide.

Topics:

- Audience
- Documentation Accessibility
- Diversity and Inclusion
- Related Resources
- Conventions

Audience

This guide is intended for developers who want to use this adapter in integrations in Oracle Integration.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and

partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

See these Oracle resources:

*   Oracle Cloud

    http://cloud.oracle.com
*   *Using Integrations in Oracle Integration Generation 2*
*   *Using the Oracle Mapper with Oracle Integration Generation 2*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Understand the Microsoft Office 365 Outlook Adapter

Review the following conceptual topics to learn about the Microsoft Office 365 Outlook Adapter and how to use it as a connection in integrations in Oracle Integration. A typical workflow of adapter and integration tasks is also provided.

Topics:

• Microsoft Office 365 Outlook Adapter Capabilities
• What Application Version Is Supported?
• About Microsoft Office 365 Outlook Adapter Use Cases
• Workflow to Create and Add a Microsoft Office 365 Outlook Adapter Connection

> **Note:**
>
> There are overall service limits for Oracle Integration. A service limit is the quota or allowance set on a resource. See Service Limits.

Microsoft Office 365 Outlook Adapter Capabilities

The Microsoft Office 365 Outlook Adapter enables you to create an integration with a Microsoft Office 365 Outlook application.

Use the Microsoft Office 365 Outlook Adapter in an Oracle Integration integration to retrieve messages in Office 365 and Outlook.com. The Microsoft Office 365 Outlook Adapter enables you to manage messages, manage folders, and so on.

The Microsoft Office 365 Outlook Adapter supports the Microsoft Graph REST API operations. Outlook Mail REST API operations have been desupported.

The Microsoft Office 365 Outlook Adapter is one of many predefined adapters included with Oracle Integration. You can configure the Microsoft Office 365 Outlook Adapter as a connection in an integration in Oracle Integration.

What Application Version Is Supported?

For information about which application version is supported by this adapter, see the Connectivity Certification Matrix.

See Connectivity Certification Matrix.

About Microsoft Office 365 Outlook Adapter Use Cases

The Microsoft Office 365 Outlook Adapter can be used in the following scenarios.

- You can integrate a Microsoft Office 365 Outlook account with the Microsoft Office 365 Outlook Adapter to return information such as emails, attachments, and folders

- You can integrate a Microsoft Office 365 Outlook account with the Microsoft Office 365 Outlook Adapter to complete tasks such as sending email, creating new folders, deleting email and attachments, and creating new file attachments.

> **✎ Note:**
>
> Oracle Integration offers a number of prebuilt integrations, known as *recipes*, that provide you with a head start in building your integrations. You can start with a recipe, and then customize it to fit your needs and requirements. Depending upon the solution provided, a variety of adapters are configured in the prebuilt integrations.
> See the Recipes and Accelerators page on the Oracle Help Center.

Workflow to Create and Add a Microsoft Office 365 Outlook Adapter Connection

Follow a workflow to create a connection with an adapter and include the connection in an integration in Oracle Integration.

Step	Description	More Information
1	Create the adapter connections for the applications you want to integrate. The connections can be reused in multiple integrations and are typically created by the administrator.	Create a Microsoft Office 365 Outlook Adapter Connection
2	Create the integration. When you do this, you add trigger and invoke connections to the integration.	Create Integrations and Add the Microsoft Office 365 Outlook Adapter Connection to an Integration
3	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in *Using Integrations in Oracle Integration Generation 2*
4	(Optional) Create lookups that map the different values used by those applications to identify the same type of object (such as gender codes or country codes).	Manage Lookups in *Using Integrations in Oracle Integration Generation 2*
5	Activate the integration.	Manage Integrations in *Using Integrations in Oracle Integration Generation 2*

Step	Description	More Information
6	Monitor the integration on the dashboard.	Monitor Integrations in *Using Integrations in Oracle Integration Generation 2*
7	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Manage Business Identifiers for Tracking Fields in Messages in *Using Integrations in Oracle Integration Generation 2*
8	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in *Using Integrations in Oracle Integration Generation 2*

2

Create a Microsoft Office 365 Outlook Adapter Connection

A connection is based on an adapter. You define connections to the specific cloud applications that you want to integrate.

Topics:

- Prerequisites for Creating a Connection
- Create a Connection
- Upload an SSL Certificate

Prerequisites for Creating a Connection

These are the prerequisites for creating a connection with the Microsoft Office 365 Outlook Adapter.

> **Note:**
>
> Before creating a Microsoft Office 365 Outlook Adapter connection, you must upload the trusted public certificate to Oracle Integration. The public certificate is created when you create the private key. Rename the public certificate file extension to `.crt`. To upload the certificate, see Upload an SSL Certificate.

1. Log in to `https://azure.microsoft.com/` with administrator access. If you do not have an account, click **Free account**.

2. In the upper right, click **Portal**.

3. In the search field at the top, enter `app registration`, then click the **Search** icon.

4. Click **New registration**.

5. In the **Name** field, enter the user-facing display name for this application.

6. In the **Supported account types** section, select **Accounts in Any Organizational Directory**.

7. In the **Redirect URI (optional)** section, select **Web**, then enter the redirect URL.

   ```
   https://instance_URL/icsapis/agent/oauth/callback
   ```

8. Click **Register**.

9. If you want to add more redirect URLs, click the link in the **Redirect URIs** section on the right side of the page.

10. In the left navigation pane, click **Certificates & secrets** to generate a secret.

11. In the **Client sections** section, click **New client secret**.

12. In the **Description** field, enter a description for the secret.

13. In the **Expires** section, select the proper expiration time (preferably **Never**).

14. Click **Add**.

15. In the **Client sections** section at the bottom, copy the client secret value in the **Value** column. This value is required when configuring the connection on the Connections page.

> **✎ Note:**
>
> The client secret value cannot be displayed again once you exit the Microsoft Azure page. Ensure that you copy this value.

16. In the left navigation pane, click **API permissions** to add required permissions to the application.

17. Click **Microsoft Graph**.

18. In the **Select permissions** field, begin entering the name of the adapter for which you are configuring permissions. For the Microsoft Office 365 Outlook Adapter, enter `Email`.
Available permissions are displayed. You enter these permissions in the **Scope** field when configuring a connection on the Connections page.

19. Select the necessary permissions, and click **Update Permissions**. The `offline_access` scope is required. This scope is needed to get a refresh token, which is then used to get new access tokens. See Scopes and permissions in the Microsoft identity platform.

20. In the left navigation pane, click **Overview**.

21. Copy the value shown in the **Application (client) ID** field. This value is required when configuring the connection on the Connections page.

Microsoft also provides an example of how to create this application. See Quickstart: Configure a client application to access web APIs.

Create a Connection

Before you can build an integration, you have to create the connections to the applications with which you want to share data.

To create a connection in Oracle Integration:

1. In the left navigation pane, click **Home** > **Integrations** > **Connections**.

2. Click **Create**.

> **Note:**
>
> You can also create a connection in the integration canvas of:
>
> - An orchestrated integration (See Define Inbound Triggers and Outbound Invokes.)
>
> - A basic routing integration (See Add a Trigger (Source) Connection.)

3. In the Create Connection — Select Adapter dialog, select the adapter to use for this connection. To find the adapter, scroll through the list, or enter a partial or full name in the **Search** field and click

   🔍

   Search.

4. In the Create Connection dialog, enter the information that describes this connection.

   a. Enter a meaningful name to help others find your connection when they begin to create their own integrations. The name you enter is automatically added in capital letters to the **Identifier** field. If you modify the identifier name, don't include blank spaces (for example, SALES OPPORTUNITY).

   b. Enter optional keywords (tags). You can search on the connection keywords on the Connections page.

   c. Select the role (direction) in which to use this connection (trigger, invoke, or both). Only the roles supported by the adapter are displayed for selection. When you select a role, only the connection properties and security policies appropriate to that role are displayed on the Connections page. If you select an adapter that supports both invoke and trigger, but select only one of those roles, you'll get an error when you try to drag the adapter into the section you didn't select. For example, let's say you configure a connection for the Oracle Service Cloud (RightNow) Adapter as only an **invoke**. Dragging the adapter to a **trigger** section in the integration produces an error.

   d. Enter an optional description of the connection.

5. Click **Create**.

   Your connection is created. You're now ready to configure the connection details, such as connection properties, security policies, connection login credentials, and (for certain connections) agent group.

Configure Connection Security

Enter connection information so your application can process requests.

1. Go to the **Security** section.

2. Enter the client ID (application ID) and client secret values you recorded when you added your application to your Microsoft Office 365 Outlook account. See Prerequisites for Creating a Connection.

3. Enter the scope URLs in the **Scope** field.

   A scope is a list of authorization permissions for the target application. You must include the offline_access scope along with the application-specific scopes. A blank space between each scope is also required. For example:

- If using the Outlook REST APIs:

  ```
  https://outlook.office.com/mail.send https://outlook.office.com/
  mail.readwrite offline_access
  ```

- If using the Microsoft Graph REST APIs:

  ```
  https://graph.microsoft.com/Mail.ReadWrite https://
  graph.microsoft.com/Mail.Send offline_access
  ```

> **✎ Note:**
>
> - You cannot use both Outlook and Microsoft Graph scopes in one connection.
> - Do not specify Outlook scopes if you plan to select a Microsoft Graph REST API operation during adapter configuration. See Error Occurs If Using Outlook Scopes with a Microsoft Graph REST API Operation.

Ensure you correctly enter your scope values. Otherwise, you receive an error when clicking **Provide Consent**.

4. Click **Provide Consent**. This enables Oracle Integration to interact with the Microsoft Office 365 Outlook account used to create the application at `https://portal.azure.com/`. If everything is correct, you are prompted for the Oracle Integration credentials.

   a. Enter the credentials and click **OK**. These are the same credentials you use to log in to Oracle Integration.

   b. Enter the Microsoft Office 365 Outlook account credentials.

      A page is displayed asking for permission to interact with the account.

   c. Click **Yes**.

      The Access Allowed! page is displayed.

Test the Connection

Test your connection to ensure that it's configured successfully.

1. In the page title bar, click **Test**. What happens next depends on whether your adapter connection uses a Web Services Description Language (WSDL) file. Only some adapter connections use WSDLs.

If Your Connection...	Then...
Doesn't use a WSDL	The test starts automatically and validates the inputs you provided for the connection.

If Your Connection...	Then...
Uses a WSDL	A dialog prompts you to select the type of connection testing to perform:
	• **Validate and Test**: Performs a full validation of the WSDL, including processing of the imported schemas and WSDLs. Complete validation can take several minutes depending on the number of imported schemas and WSDLs. No requests are sent to the operations exposed in the WSDL.
	• **Test**: Connects to the WSDL URL and performs a syntax check on the WSDL. No requests are sent to the operations exposed in the WSDL.

2. Wait for a message about the results of the connection test.

   • If the test was successful, then the connection is configured properly.

   • If the test failed, then edit the configuration details you entered. Check for typos, verify URLs and credentials, and download the diagnostic logs for additional details. Continue to test until the connection is successful.

3. When complete, click **Save**.

Upload an SSL Certificate

Certificates are used to validate outbound SSL connections. If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception is thrown. In that case, you must upload the appropriate certificate. A certificate enables Oracle Integration to connect with external services. If the external endpoint requires a specific certificate, request the certificate and then upload it into Oracle Integration.

To upload an SSL certificate:

1. In the left navigation pane, click **Home** > **Settings** > **Certificates**.
   All certificates currently uploaded to the trust store are displayed in the Certificates dialog. The

   link enables you to filter by name, certificate expiration date, status, type, category, and installation method (user-installed or system-installed). Certificates installed by the system cannot be deleted.

2. Click **Upload** at the top of the page.
   The Upload Certificate dialog box is displayed.

3. Enter an alias name and optional description.

4. In the **Type** field, select the certificate type. Each certificate type enables Oracle
   Integration to connect with external services.

   - **X.509 (SSL transport)**

   - **SAML (Authentication & Authorization)**

   - **PGP (Encryption & Decryption)**

X.509 (SSL transport)

1. Select a certificate category.

   a. **Trust**: Use this option to upload a trust certificate.

      i. Click **Browse**, then select the trust file (for example, `.cer` or `.crt`) to
         upload.

   b. **Identity**: Use this option to upload a certificate for two-way SSL
      communication.

      i. Click **Browse**, then select the keystore file (`.jks`) to upload.

      ii. Enter the comma-separated list of passwords corresponding to key
          aliases.

      > **Note:**
      >
      > When an identity certificate file (JKS) contains more than one
      > private key, all the private keys must have the same password. If
      > the private keys are protected with different passwords, the
      > private keys cannot be extracted from the keystore.

      iii. Enter the password of the keystore being imported.

   c. Click **Upload**.

SAML (Authentication & Authorization)

1. Note that **Message Protection** is automatically selected as the only available
   certificate category and cannot be deselected. Use this option to upload a keystore
   certificate with SAML token support. Create, read, update, and delete (CRUD)
   operations are supported with this type of certificate.

2. Click **Browse**, then select the certificate file (`.cer` or `.crt`) to upload.

3. Click **Upload**.

PGP (Encryption & Decryption)

1. Select a certificate category. Pretty Good Privacy (PGP) provides cryptographic
   privacy and authentication for communication. PGP is used for signing, encrypting,
   and decrypting files. You can select the private key to use for encryption or
   decryption when configuring the stage file action.

   a. **Private**: Uses a private key of the target location to decrypt the file.

     i.   Click **Browse**, then select the PGP file to upload.

     ii. Enter the PGP private key password.

b. **Public**: Uses a public key of the target location to encrypt the file.

     i.   Click **Browse**, then select the PGP file to upload.

     ii. In the **ASCII-Armor Encryption Format** field, select **Yes** or **No**. **Yes** shows the format of the encrypted message in ASCII armor. ASCII armor is a binary-to-textual encoding converter. ASCII armor formats encrypted messaging in ASCII. This enables messages to be sent in a standard messaging format. This selection impacts the visibility of message content. **No** causes the message to be sent in binary format.

     iii. From the **Cipher Algorithm** list, select the algorithm to use. Symmetric-key algorithms for cryptography use the same cryptographic keys for both encryption of plain text and decryption of cipher text.

c. Click **Upload**.

3

Add the Microsoft Office 365 Outlook Adapter Connection to an Integration

When you drag the Microsoft Office 365 Outlook Adapter into the invoke area of an integration, the Adapter Endpoint Configuration Wizard appears. This wizard guides you through configuration of Microsoft Office 365 Outlook Adapter endpoint properties.

These topics describe the wizard pages that guide you through configuration of the Microsoft Office 365 Outlook Adapter as an invoke in an integration. The Microsoft Office 365 Outlook Adapter cannot be used as a trigger in an integration.

Topics:

- Basic Info Page
- Invoke Operations Page
- Summary Page

Basic Info Page

You can enter a name and description on the Basic Info page of each adapter in your integration.

Element	Description
What do you want to call your endpoint?	Provide a meaningful name so that others can understand the responsibilities of this connection. You can include English alphabetic characters, numbers, underscores, and hyphens in the name. You can't include the following characters:
	• No blank spaces (for example, `My Inbound Connection`)
	• No special characters (for example, `#;83&` or `righ(t)now4`) except underscores and hyphens
	• No multibyte characters
What does this endpoint do?	Enter an optional description of the connection's responsibilities. For example:
	`This connection receives an inbound request to synchronize account information with the cloud application.`

Invoke Operations Page

Select the Microsoft Office 365 Outlook API operation to perform.

> **✏ Note:**
>
> The Microsoft Office 365 Calendar Adapter supports the selection of Microsoft Graph REST API operations from the **Select Operation** list. The Outlook Mail REST API operations have the same names and are still available for selection, but are identified as **Desupported** in the **Select Operation** list.

Operation	Description
Get folders	Returns a folder collection or an individual folder from a mailbox.
Create a folder	Creates a folder in a mailbox.
Delete a message	Deletes a message in a mailbox.
Delete attachments	Returns a message collection or an individual message from a mailbox folder.
Send a new message	Creates and sends a new message.
Reply to a message	Returns a response to a message.
Forward a message	Forwards a message to a mailbox.
Get messages	Returns a message collection or an individual message from a mailbox folder.
Get messages of a folder	Returns a message collection or an individual message from a specific folder.
Move a message	Moves a message collection or an individual message from one mailbox folder to another.
Copy a message	Copies a message collection or an individual message from one mailbox folder to another.
Get an attachment collection	Returns a collection of attachments from a mailbox folder.
Get an attachment	Returns an individual attachment from a mailbox folder.
Create a file attachment	Creates an attachment and attaches it to a message in a mailbox folder.

Summary Page

You can review the specified adapter configuration values on the Summary page.

Element	Description
Summary	Displays a summary of the configuration values you defined on previous pages of the wizard.
	The information that is displayed can vary by adapter. For some adapters, the selected business objects and operation name are displayed. For adapters for which a generated XSD file is provided, click the XSD link to view a read-only version of the file.
	To return to a previous page to update any values, click the appropriate tab in the left panel or click **Back**.
	To cancel your configuration details, click **Cancel**.

4
Troubleshoot the Microsoft Office 365 Outlook Adapter

Review these topics to learn about troubleshooting issues with the Microsoft Office 365 Outlook Adapter.

Topics:

- Error Occurs If Using Outlook Scopes with a Microsoft Graph REST API Operation
- Expired Refresh Token Causes an Invalid Token Error
- Unauthorized Security Setup
- Specify the Port Number with the Authorized Redirect URL
- ContentType Passed in the Request Body Must Either be Text or HTML

Additional integration troubleshooting information is provided. See Troubleshoot Oracle Integration in *Using Integrations in Oracle Integration Generation 2* and the Oracle Integration Troubleshooting page on the Oracle Help Center.

Error Occurs If Using Outlook Scopes with a Microsoft Graph REST API Operation

The Connections page currently provides Outlook scope examples in the **Scope** field. If you try to configure a new connection with an Outlook scope, then select a Microsoft Graph REST API operation in the Adapter Endpoint Configuration Wizard, you receive a `401` error during runtime.

If you want to use a Microsoft Graph REST API operation, ensure that you select a Microsoft Graph scope during connection configuration. See Configure Connection Security.

Expired Refresh Token Causes an Invalid Token Error

The refresh token expires after 90 days of inactivity. Microsoft also reserves the right to expire the token at any time for security reasons. The following error message indicates that a refresh token has expired and cannot be exchanged for a new token.

```
<genericRestFault><errorCode>400</errorCode><errorPath><![CDATA[POST
https://login.microsoftonline.com/common/oauth2/v2.0/token returned a
response
status of 400 Bad Request]]></errorPath><instance><!
[CDATA[{"error":"invalid_grant",
"error_description":"AADSTS700082: The refresh token has expired due to
inactivity.
The token was issued on 2019-11-05T19:11:55.7631194Z and was inactive for
90.00:00:00.
\r\nTrace ID: b7b09af0-2391-4840-93ee-59b383031700\r\nCorrelation ID:
```

```
16ff8fa7-e78c-499a-b4f5-c18498b94f6c\r\nTimestamp: 2020-03-12
01:41:39Z",
. . .
. . .
. . .
```

If the refresh token has expired, perform the following steps:

1. Click **Provide Consent** again on the Connections page for the Microsoft Office 365 Outlook Adapter connection and go through the OAuth process.
    After completing this process, a new token is acquired.

2. Test and save the connection.
    After this, the token is renewed and the connection works as expected.

See Configurable token lifetimes in Azure Active Directory.

Unauthorized Security Setup

This issue occurs when an API request is made without access tokens. When an API request is submitted without access tokens, the error message `Unauthorized!! Security setup not done for account` is displayed.

Reset the Microsoft Office 365 Outlook Security Credentials

Solution: Repeat the procedure for setting the Microsoft Office 365 Outlook security credentials. See Configure Connection Security.

If resetting the email security credentials does not resolve the error message, make sure REST API functionality is enabled on the Microsoft Office 365 Outlook account and the scopes defined for the connection are correct. See Prerequisites for Creating a Connection and Configure Connection Security.

Specify the Port Number with the Authorized Redirect URL

When configuring the authorized redirect URL, ensure that you specify the port number. For example:

```
https://host:443/icsapis/agent/oauth/callback
```

Not specifying the port number in the URL results in an error saying the application wasn't authorized for the redirect URL.

ContentType Passed in the Request Body Must Either be Text or HTML

As per the Microsoft documentation, the `ContentType` value passed in the request `Body` can either be `Text` or `HTML`.

Any other value passed in the request results in an error from Microsoft Office 365 Outlook such as the following:

```
POST https://outlook.office.com/api/v2.0/me/sendmail returned a response
status of 400 Bad Request
```

```
{"error":{"code":"RequestBodyRead","message":"Requested value 'text/xml' was
not found."}}
```