Oracle® Cloud

Using the Mailchimp Adapter with Oracle Integration 3

F45562-05
November 2025

Oracle Cloud Using the Mailchimp Adapter with Oracle Integration 3,

F45562-05

Primary Author: Oracle Corporation

Contents

About This Content

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

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.

Related Resources

See these Oracle resources:

- Oracle Cloud at `http://cloud.oracle.com`
- *Using Integrations in Oracle Integration 3*
- *Using the Oracle Mapper with Oracle Integration 3*
- Oracle Integration documentation on the Oracle Help Center.

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 Mailchimp Adapter

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

Topics:

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

Mailchimp Adapter Capabilities

The Mailchimp Adapter enables you to connect to Mailchimp REST APIs from Oracle Integration.

Mailchimp is an email marketing software (EMS) program that provides options for designing, sending, and saving email templates. You can create newsletters and share them on social network sites such as Twitter or Facebook. You can build a list of contacts with whom you want to market products, and save the list for later use. You can also create custom templates for your products so that you do have to rewrite emails.

The Mailchimp Adapter is one of the many predefined adapters included with Oracle Integration. You can configure the Mailchimp 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.

About Mailchimp Adapter Use Cases

The Mailchimp Adapter can be used in the following scenarios.

- You can integrate the Mailchimp Adapter with information technology service applications to generate mailing and contact lists.
- You can integrate the Mailchimp Adapter with marketing applications to generate marketing emails.

- You can configure the Mailchimp Adapter to return client information and statistics including the average number of clicks made in a campaign and the number of campaign emails opened by clients.

> **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 Mailchimp Adapter Connection to an Integration

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

This table lists the workflow steps for both adapter tasks and overall integration tasks, and provides links to instructions for each workflow step.

Step	Description	More Information
1	Decide where to work	• Work in a project (see why working with projects is preferred in *Using Integrations in Oracle Integration 3*). • Work outside a project.
2	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 Mailchimp Adapter Connection
3	Create the integration. When you do this, you add trigger and invoke connections to the integration.	Understand Integration Creation and Best Practices in *Using Integrations in Oracle Integration 3* and Add the Mailchimp Adapter Connection to an Integration
4	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in *Using Integrations in Oracle Integration 3*
5	(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 3*
6	Activate the integration.	Manage Integrations in *Using Integrations in Oracle Integration 3*
7	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in *Using Integrations in Oracle Integration 3*
8	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Track Integration Instances in *Using Integrations in Oracle Integration 3*

Step	Description	More Information
9	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in *Using Integrations in Oracle Integration 3*

2

Create a Mailchimp 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

Before you create the Mailchimp Adapter connection, you need to create a Mailchimp account and add the application. You can use an existing Mailchimp account, but you need to add the application to create a connection. Use this procedure to create a new Mailchimp account and add the application.

> **Note**
>
> To create a connection, a trusted Mailchimp public certificate is required. Typically, the certificate is included with Oracle Integration. If you cannot locate the Mailchimp public certificate, download it from https://login.mailchimp.com/oauth2/metadata. Rename the public certificate file extension to `.crt`. To upload the certificate, see Upload a Certificate to Connect with External Services.

1. Open a web browser and browse to the Mailchimp web site (http://mailchimp.com).
2. Click **Sign up Free**.
3. Enter your email address, user name, and password.
4. Click **Create My Account**.
5. Activate your account following the instructions in the Mailchimp confirmation email.
6. Complete the Let's Get Started page.
7. Click **Save and Get Started**.
8. Click your user name in the upper right corner and select **Account.**
9. Click **Extras** and then select **API keys**.
10. Click **Register and Manage Your Apps**.
11. Click **Register An App**.
12. Complete the **Register an App** fields. Enter the URL in the **Redirect URI** field.

> **Note**
>
> If you don't know the following information, check with your administrator:
>
> - If your instance is new or upgraded from Oracle Integration Generation 2 to Oracle Integration 3.
> - The complete instance URL with the region included (required for new instances).

For Connections…	Include the Region as Part of the Redirect URL?	Example of Redirect URL to Specify…
Created on new Oracle Integration 3 instances	Yes.	`https://`*`OIC_instance_URL`*`.`*`region`*`.ocp.oraclecloud.com/icsapis/agent/oauth/callback`
Created on instances upgraded from Oracle Integration Generation 2 to Oracle Integration 3	No. This applies to both: • New connections created after the upgrade • Existing connections that were part of the upgrade	`https://`*`OIC_instance_URL`*`.ocp.oraclecloud.com/icsapis/agent/oauth/callback`

13. Click **Create**.
14. Copy or record the values in the **Client ID** and **Client secret** fields. These values are required to create the connection in Oracle Integration.

Create a Connection

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

> **Note**
>
> You can also create a connection in the integration canvas. See Define Inbound Triggers, Outbound Invokes, and Actions.

To create a connection in Oracle Integration:

1. Decide where to start:
   - Work in a project (see why working with projects is preferred).
     a. In the navigation pane, click **Projects**.
     b. Select the project name.
     c. Click **Integrations**.

d. In the **Connections** section, click **Add** if no connections currently exist or **+** if connections already exist. The Create connection panel opens.

- Work outside a project.
  a. In the navigation pane, click **Design**, then **Connections**.
  b. Click **Create**. The Create connection panel opens.

2. 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.
3. Enter the information that describes this connection.

Element	Description
Name	Enter a meaningful name to help others find your connection when they begin to create their own integrations.
Identifier	Automatically displays the name in capital letters that you entered in the **Name** field. If you modify the identifier name, don't include blank spaces (for example, `SALES_OPPORTUNITY`).
Role	Select the role (direction) in which to use this connection. **Note**: *Only* the roles supported by the adapter you selected are displayed for selection. Some adapters support all role combinations (trigger, invoke, or trigger and invoke). Other adapters support fewer role combinations. 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, assume 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.
Keywords	Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
Description	Enter an optional description of the connection.

Element	Description
Share with other projects	**Note**: This field only appears if you are creating a connection in a project. Select to make this connection publicly available in other projects. Connection sharing eliminates the need to create and maintain separate connections in different projects. When you configure an adapter connection in a different project, the **Use a shared connection** field is displayed at the top of the Connections page. If the connection you are configuring matches the same type and role as the publicly available connection, you can select that connection to reference (inherit) its resources. See Add and Share a Connection Across a Project.

4. Click **Create**.

   Your connection is created. You're now ready to configure the connection properties, security policies, and (for some connections) access type.

5. Follow the steps to configure a connection.
   The connection property and connection security values are specific to each adapter. Your connection may also require configuration with an access type such as a private endpoint or an agent group.

6. Test the connection.

Configure Connection Security

Enter connection information so your application can process requests.

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

   The **Security Policy** field displays **MailchimpSecurityPolicy** by default. This field cannot be changed.

2. Enter the client ID and client secret values you recorded when you created your Mailchimp account.

   See Prerequisites for Creating a Connection.

3. Click **Provide Consent**.
4. If required, enter your Mailchimp user name and password.
5. Click **Log In**.
6. Return to Oracle Integration to test and save the security credentials.

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.
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 and verify URLs and credentials. Continue to test until the connection is successful.
3. When complete, click **Save**.

Upload a Certificate to Connect with External Services

Certificates allow Oracle Integration to connect with external services. If the external service/endpoint needs a specific certificate, request the certificate and then import it into Oracle Integration.

If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception error 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.

1. Sign in to Oracle Integration.
2. In the navigation pane, click **Settings**, then **Certificates**.
   All certificates currently uploaded to the trust store are displayed on the Certificates page.
3. Click **Filter** to filter by certificate expiration date, status, and type. Certificates installed by the system cannot be deleted.
4. Click **Upload** at the top of the page.
   The Upload certificate panel is displayed.
5. Enter an alias name and optional description.
6. In the **Type** field, select the certificate type. Each certificate type enables Oracle Integration to connect with external services.
   - Digital Signature
   - X.509 (SSL transport)
   - SAML (Authentication & Authorization)
   - PGP (Encryption & Decryption)
   - Signing key

Digital Signature

The digital signature security type is typically used with adapters created with the Rapid Adapter Builder. See Learn About the Rapid Adapter Builder in Oracle Integration in *Using the Rapid Adapter Builder with Oracle Integration 3*.

1. Click **Browse** to select the digital certificate. The certificate must be an X509Certificate. This certificate provides inbound RSA signature validation. See RSA Signature Validation in *Using the Rapid Adapter Builder with Oracle Integration 3*.
2. Click **Upload**.

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. The following supported cipher algorithms are FIPS-compliant:

- AES128
- AES192
- AES256
- TDES

c. Click **Upload**.

Signing key

A signing key is a secret key used to establish trust between applications. Signing keys are used to sign ID tokens, access tokens, SAML assertions, and more. Using a private signing key, the token is digitally signed and the server verifies the authenticity of the token by using a public signing key. You must upload a signing key to use the OAuth Client Credentials using JWT Client Assertion and OAuth using JWT User Assertion security policies in REST Adapter invoke connections. Only PKCS1- and PKCS8-formatted files are supported.

1. Select **Public** or **Private**.
2. Click **Browse** to upload a key file.
   If you selected **Private**, and the private key is encrypted, a field for entering the private signing key password is displayed after key upload is complete.
3. Enter the private signing key password. If the private signing key is not encrypted, you are not required to enter a password.
4. Click **Upload**.

3

Add the Mailchimp Adapter Connection to an Integration

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

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

Topics:

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

Enter the Mailchimp Adapter invoke operation values for your integration.

The following table describes the available Mailchimp API operations on the Mailchimp Adapter page. Select the operation to perform.

Operation	Description
Get member info	Returns a list of members that are of a particular status and potentially matching a segment.
Get interest categories of a list	Returns all interest categories for a defined mailing list.
Get all lists	Returns all of the lists defined for a user account.
Get all segments in a list	Returns all segments defined for a subscriber list.
Get top email clients	Returns a list of the most active subscribers and ranks the clients by popularity.
Get all campaign folders	Returns a list of all campaign folders for a user account.
Create Campaign Folder	Creates a campaign folder.
Get all campaigns	Returns a the list of all existing campaigns and their details.
Send a campaign	Sends a campaign email to the specified email addresses.
Create a new campaign	Creates a new campaign.
Create a new interest category	Creates a new interest category for a subscription list.
Get a specific campaign folder	Returns a specific campaign folder.
Delete a specific campaign folder	Deletes a specific campaign folder.
Create a new segment	Creates a new segment.

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 **Go back**. To cancel your configuration details, click **Cancel**.

4

Troubleshoot the Mailchimp Adapter

Review these topics to learn about troubleshooting issues with the Mailchimp Adapter .

Topics:

Mailchimp Website Authentication Error

This issue occurs when you click **Provide Consent** on the Connections page and the redirect URL cannot be authenticated.

Update the Mailchimp redirect URL

Solution: Use this procedure to update the Mailchimp redirect URL.

1. Open a web browser and browse to the Mailchimp web site (http://mailchimp.com).
2. Click **Log In**.
3. Enter your user name and password.
4. Click **Log In**.
5. Click your user name in the upper right corner and select **Account**.
6. Click **Extras** and then select **API keys**.
7. Click **Register and Manage Your Apps**.
8. Click **Edit** on the application you want to update.
9. Update the **Redirect URI** field.
10. Click **Update**.
11. Click your user name in the upper right corner and select **Log Out**.

See Configure Connection Security.

SSL Error When Providing Consent

This issue occurs when you click **Provide Consent** in the Credentials dialog and the public certificate is missing or cannot be located.

Upload the Mailchimp public certificate to Oracle Integration

Solution: Upload the Mailchimp public certificate to Oracle Integration. To upload the certificate, see Upload a Certificate to Connect with External Services.

To specify security credentials, see Configure Connection Security.