Oracle® Cloud

Using the Twitter Adapter with Oracle Integration 3

F45615-02
April 2024

ORACLE

Oracle Cloud Using the Twitter Adapter with Oracle Integration 3,

F45615-02

Primary Author: Oracle Corporation

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

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 `https://www.oracle.com/corporate/accessibility/`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `https://support.oracle.com/portal/` or visit `Oracle Accessibility Learning and Support` 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 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 Twitter Adapter

Review the following conceptual topics to learn about the Twitter 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:

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

Twitter Adapter Capabilities

The Twitter Adapter enables you to create an integration with a Twitter application. Twitter is an online social networking service that enables you to send and read short messages called tweets. If you register with Twitter, you can read and post tweets. If you do not log in, you can only read tweets.

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

Workflow to Create and Add a Twitter Adapter Connection to an Integration

You follow a very simple 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 Twitter Adapter Connection
2	Create the integration. When you do this, you add trigger and invoke connections to the integration.	Create Integrations and Add the Twitter 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 3*
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 3*
5	Activate the integration.	Manage Integrations in *Using Integrations in Oracle Integration 3*
6	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in *Using Integrations in Oracle Integration 3*
7	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*
8	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 Twitter 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

To use the Twitter Adapter, you must first have access to the Twitter API for your integration. To access the Twitter API, you must create an application.

To create an application:

> **Note:**
>
> Create a separate Twitter application for every Oracle Integration instance.

1. Go to the Twitter developer page at https://dev.twitter.com.
2. Create a new account or log in using an existing account if you already have one.
3. Click **Manage Your Apps** in the footer of the Twitter developer page.
4. Create a new application or select an existing one if already created.
5. Authorize your application to use your Twitter account by clicking **Create my access token**.
6. On the **Permissions** tab, ensure that the application has **Read and Write** permissions.
7. Copy and paste the OAuth settings to a safe location, as displayed in the **Keys and Access Tokens** tab.

   You need the following information. These keys contain sensitive data, and must be kept secret. If anyone gets this information, they can access your Twitter account.

   - Consumer key
   - Consumer secret
   - Access token
   - Access token secret

   You specify this information when creating a connection in Configure Connection Security.

> **Note:**
>
> Before creating a Twitter connection, you must upload the trusted Twitter public certificate to Oracle Integration. The Twitter public certificate can be downloaded from https://twitter.com. Rename the public certificate file extension to `.cer`. See Upload a Certificate to Connect with External Services.

Create a Connection

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

To create a connection in Oracle Integration:

1. In the navigation pane, click **Design**, then **Connections**.
2. Click **Create**.

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

3. In the Create connection panel, 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.
4. 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`).

Element	Description
Role	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, 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.
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.

5. Click **Create**.

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

Configure Connection Security

Configure security for your Twitter connection by selecting the security policy and specifying the consumer key, consumer secret, access token, and access secret. The security policy grants you authorization access to the resources of the Twitter application.

1. Go to the **Security** section.
2. In the **Security Policy** field, note that the **Custom Security Policy** security policy is displayed by default, and cannot be deselected.

3. Complete the following fields with information created after completing the steps in Prerequisites for Creating a Connection.
   a. In the **Consumer Key** field, enter the consumer key.
   b. In the **Consumer Secret** field, enter the consumer secret.
   c. In the **Access Token** field, enter the access token.
   d. In the **Access Secret** field, enter the access token secret.

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

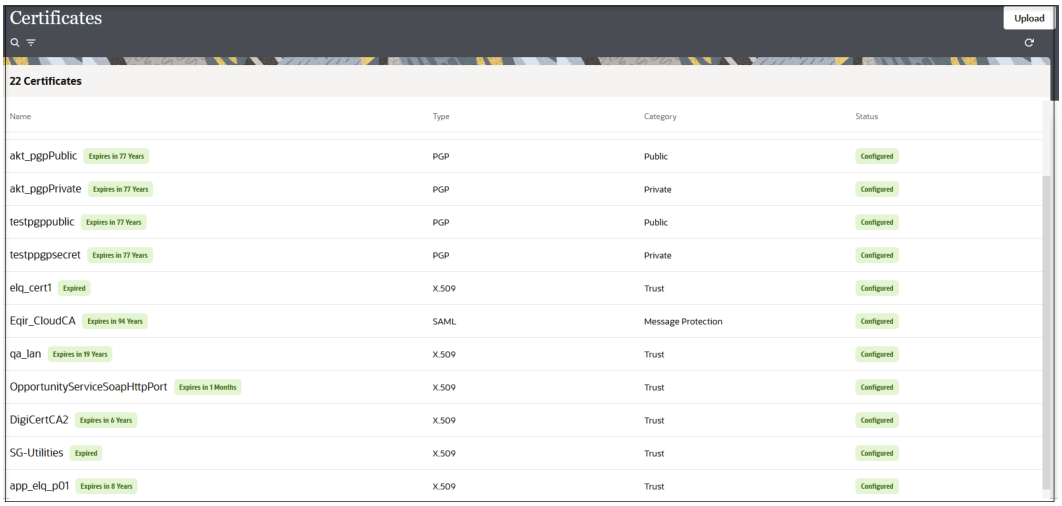
Certificates allow Oracle Integration to connect with external services. If the external service/endpoint needs a specific certificate, request the certificate and then import it into Oracle Integration.

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 name, certificate expiration date, status, type, category, and installation method (user-installed or system-installed). 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 Implement Digital Signature Validation (RSA) 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 Twitter Adapter Connection to an Integration

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

The following sections describe the wizard pages that guide you through configuration of the Twitter Adapter as an invoke in an integration. The Twitter 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 Operation Page

Select the Twitter API operation to perform.

Element	Description
Select Operation	Select the Twitter API operation to invoke. Place your cursor over each operation to view a description of the operation. • **Search Tweets** • **Get Followers IDs** • **Get IDs of Retweeters** • **Retweet** • **Tweet** • **Get Friends IDs** • **Get Trends for Place** • **Get Subscribers for List** • **Get Followers List** • **Get Retweets of Me** • **Get Friends List** • **Lookup Statuses** • **Get Trends Available**

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 Twitter Adapter

Review the following topics to learn about troubleshooting issues with the Twitter Adapter.

Topics:

Changes that Can Invalidate Credentials Required for the Twitter Connection

There are circumstances that can invalidate the Twitter credentials.

Regenerating your consumer key and consumer secret (by clicking on 'Regenerate Consumer Key and Secret' button for your app on the Twitter developer site).

Solution: Update the Twitter Adapter connection in Oracle Integration with the new values for consumer key, consumer secret, access token, and access token secret.

Regenerate the access token and secret for your account (by clicking on 'Regenerate My Access Token and Access Secret' button for your app on the Twitter developer site)

Solution: Update the Twitter Adapter connection in Oracle Integration with the new values for consumer key, consumer secret, access token, and access token secret.

Revoke access to your app (by clicking on 'Revoke access' and revoking access to this app on the Twitter developer site)

Solution:

1. Log in to the Twitter developer site and go to https://apps.twitter.com. Click the application name, and go to the **Keys and Access Tokens** tab.
2. Click **Create my access token** to authorize this application to access your Twitter account.
3. Update the Twitter Adapter connection in Oracle Integration with the new values of consumer key, consumer secret, access token, and access token secret.

Get an Invalid or Expired Token Error Response

The following error can occur if you have regenerated tokens or revoked access to your Twitter application.

```
Error code 89 : message : Invalid or Expired Token
```

Solution: Check the authorization for your application on the Twitter developer page and update the credentials for the adapter.

1. Log in to the Twitter developer page and go to https://apps.twitter.com.
2. If you have revoked access to the application, provide access by clicking **Generate Access Token**.
3. Make a note of the following tokens in the **Keys and Access Tokens** tab:
   - Consumer key
   - Consumer secret
   - Access token
   - Access token secret
4. Update the Twitter Adapter connection with these credentials.