Oracle® Cloud

Using the Adobe Sign Adapter with Oracle Integration 3

F45544-04
April 2024

Oracle Cloud Using the Adobe Sign Adapter with Oracle Integration 3,

F45544-04

Primary Author: Oracle Corporation

Contents

Preface

1 Understand the Adobe Sign Adapter

2 Create an Adobe Sign Adapter Connection

3 Add the Adobe Sign Adapter Connection to an Integration

4 Troubleshoot the Adobe Sign Adapter

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 `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 Adobe Sign Adapter

Review the following conceptual topics to learn about the Adobe Sign 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:

- Adobe Sign Adapter Capabilities
- What Application Version Is Supported?
- About Adobe Sign Adapter Use Cases
- Workflow to Create and Add an Adobe Sign Adapter Connection to an Integration

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

Adobe Sign Adapter Capabilities

The Adobe Sign Adapter enables you to prepare and send documents to Adobe Sign for review and approval.

The Adobe Sign Adapter integrates your applications with Adobe Document Cloud. You can replace your paper and ink signature processes with fully automated electronic signature workflows. Use a browser or mobile device to send, sign, track, and manage the review and signature process.

The Adobe Sign Adapter is one of many predefined adapters included with Oracle Integration. You can configure the Adobe Sign Adapter 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 Adobe Sign Adapter Use Cases

The Adobe Sign Adapter can be used in scenarios such as the following.

- In integration one:
  1. Select the Send Agreement for Signature operation in one integration to send an agreement for review and signing.

2. Select and configure the REST Adapter as the trigger.
3. Perform appropriate data mapping between the REST Adapter and Adobe Sign Adapter in the mapper.
4. Invoke the integration endpoint with a REST client to send a POST request to the REST Adapter.
   The Adobe Sign Adapter sends the data as a payload while invoking the configured operation in Adobe Sign.

- In integration two:
  1. Select the Get Agreement Form Data operation in the other integration to retrieve the data entered by a user when they completed the interactive agreement form fields and signed the agreement.
  2. Perform appropriate data mapping between the REST Adapter and Adobe Sign Adapter in the mapper.
     The REST Adapter sends a GET request to the Adobe Sign Adapter, which returns the form data and the signed agreement.

> **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 an Adobe Sign Adapter Connection to an Integration

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 an Adobe Sign Adapter Connection
2	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 Adobe Sign 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*

Step	Description	More Information
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 an Adobe Sign 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 a Certificate to Connect with External Services

Prerequisites for Creating a Connection

These are the prerequisites for creating a connection with the Adobe Sign Adapter.

- Obtain the Client ID and Client Secret
- Obtain the Subdomain

Obtain the Client ID and Client Secret

> **Note:**
>
> To create a connection, a trusted public certificate is required. Typically, the certificate is included with Oracle Integration. If you cannot locate the public certificate, contact your administrator. If you download a public certificate, rename the file extension to `.crt`. See Upload a Certificate to Connect with External Services.

1. Create an Adobe Document Cloud Account. If you do not have an account, you can create one here: https://acrobat.adobe.com/us/en/documents/trial-global.html.
2. Log in to your Adobe Document Cloud Account.
3. Click your user name in the upper right corner and select **My Profile**.
4. Expand **Acrobat Sign API** in the left pane and select **API Applications**.
5. Create a new application:
   - Click the **Create** icon in the upper right corner.
   - Enter a name and a display name for your application.
   - Select **PARTNER**.
   - Click **Save**.
6. Select the application you created in step 5.
7. Click **Configure OAuth for Application**.

8. Enter the redirect URL based on the state of your instance 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`

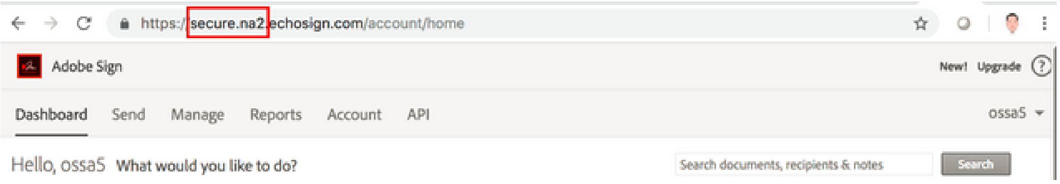
Created on instances upgraded from Oracle Integration Generation 2 to Oracle Integration 3	No.
	This applies to both:
	• New connections created after the upgrade
	• Existing connections that were part of the upgrade
		`https://`
		`OIC_instance_URL``.ocp.oraclecloud.com/icsapis/agent/oauth/callback`

9. Enable the **user_login**, **agreement_read**, **agreement_write**, **agreement_send**, and **library_read** scopes.
10. Select the **account** modifier for the **user_login**, **agreement_read**, **agreement_write**, **agreement_send**, and **library_read** scopes.
11. Copy or record the values in the **Client ID** and **Client Secret** fields. These values are required to create the connection in Oracle Integration. See Configure Connection Security.
12. Click **Save**.

Obtain the Subdomain

To create a connection, you can optionally provide the subdomain.

1. Log in to the Dashboard.
2. Go to the **Dashboard** tab.
3. Copy the domain name. An example of the **Dashboard** tab with a domain name of `secure.na2` is shown below.


https://secure.na2echosign.com/account/home
Adobe Sign
New! Upgrade
Dashboard
Send
Manage
Reports
Account
API
ossa5
Hello, ossa5 What would you like to do?
Search documents, recipients & notes
Search

See Configure Connection Security.

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`).
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.

Element	Description
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

Enter connection information so your application can process requests.

1. Go to the **Properties** section.

   The **Security Policy** field displays **AdobeSign OAuth Authorization Code Credentials**. This value cannot be changed. This policy supports the OAuth 2.0 framework and three-legged authentication.

2. Enter the subdomain of the authentication URL. The subdomain can be copied from the browser address after logging in to your Dashboard. For example:

   - `oracle.na1`
   - `ge.na1`
   - `google.na1`
   - `secure.na2`

   A URL is automatically assembled from the subdomain you specify. For example, `https://oracle.na1.echosign.com/public/oauth/v2`.

   If you do not enter a subdomain in this field, `https://secure.echosign.com/public/oauth/v2` is used by default.

   See Prerequisites for Creating a Connection.

3. Enter the client ID and client secret values you recorded when you created your Adobe Document Cloud Account application.

   See Prerequisites for Creating a Connection.

4. Enter the scope values in the **Scope** field.

A scope is a list of authorization permissions for the target application.

5. Click **Provide Consent**.
6. If required, enter your Adobe Document Cloud Account user name and password.
7. Click **Log In**.
8. 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**.

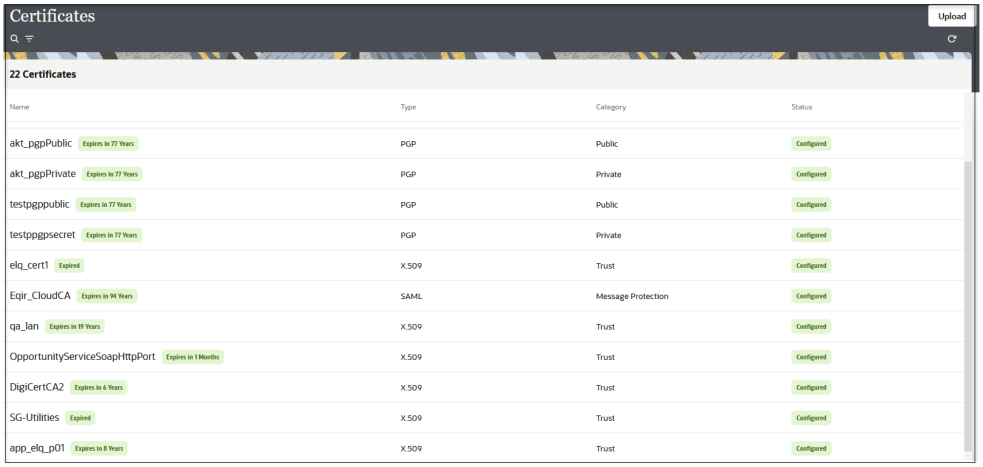
Upload a Certificate to Connect with External Services

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



22 Certificates

Name	Type	Category	Status
akt_pgpPublic Expires in 77 Years	PGP	Public	Configured
akt_pgpPrivate Expires in 77 Years	PGP	Private	Configured
testpgppublic Expires in 77 Years	PGP	Public	Configured
testppgpsecret Expires in 77 Years	PGP	Private	Configured
elq_cert1 Expired	X.509	Trust	Configured
Eqir_CloudCA Expires in 94 Years	SAML	Message Protection	Configured
qa_lan Expires in 19 Years	X.509	Trust	Configured
OpportunityServiceSoapHttpPort Expires in 1 Months	X.509	Trust	Configured
DigiCertCA2 Expires in 6 Years	X.509	Trust	Configured
SG-Utilities Expired	X.509	Trust	Configured
app_elq_p01 Expires in 8 Years	X.509	Trust	Configured

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 Adobe Sign Adapter Connection to an Integration

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

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

Topics:

- Basic Information Page
- Invoke Operations Page
- Invoke Query Page
- Summary Page

Basic Information Page

You can enter a name and description on the Basic Info page of each trigger and invoke 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 dashes in the name. You cannot include the following: • Blank spaces (for example, `My Inbound Connection`) • Special characters (for example, `#;83&` or `righ(t)now4`) • 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 Adobe Sign Adapter invoke operation values for your integration.

The table provides definitions for the Adobe Sign API operations that can be performed on the invoke connection. These operations are listed on the Adobe Sign Adapter Operations page.

Operation	Description
Send Agreement for Signature	Creates an agreement and then sends it for a signature.
Get Agreement List for User	Returns a list of agreements for a specific user.
Get Agreement Status	Returns the latest status of a specific agreement.
Get Document Ids of Agreement	Returns the IDs of the primary and supporting documents for a specific agreement.
Get Document URL	Returns the URL of a specific document.
Cancel an Agreement	Cancels an agreement and changes its status to cancel.
Delete an Agreement	Deletes all documents associated with an agreement.
Get document of an agreement	Returns the file stream of a document of an agreement.
Get information of the documents associated with an agreement	Returns a single, combined PDF document for the documents associated with an agreement.
Get agreement form data	Returns the data entered by the user into interactive form fields when they signed the agreement.
Get the audit trail of an agreement	Returns the audit trail of an agreement identified by the agreement ID.
Upload a document	Uploads a document and obtains returns the ID of the document.
Get User Workflows	Returns workflows for a user.
Get details of a Workflow	Returns the details of a workflow.
Create and Send an agreement out for signature	Creates an agreement, sends it for signatures, and returns the agreement ID in the response to the client.
Send Agreement for signature to multiple recipients	Sends an agreement to multiple recipients for their signature. Each recipient is sent a copy of the agreement for review and authorization.

Element	Description
Select Operation	Select the API operation to perform.

Invoke Query Page

Enter the Adobe Sign Adapter query parameters.

You can configure the request query parameters on the Adobe Sign Adapter Request Parameters page. This page is displayed when you select an operation that includes request parameters. The parameters that are displayed are dependent on the operation selected. For example, the parameters in the table are available for the operation `Get agreement list of the user`.

Parameter	Description
`query`	Identifies the search query string.
`externalNamespace`	Identifies the external namespace for which information should be returned.
`externalID`	Identifies the external ID for which information should be returned.
`externalGroup`	Identifies the external group for which information should be returned.

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 Adobe Sign Adapter

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

Topics:

Cause of an invalid request Error

If you receive an `invalid request` error, the redirect URI isn’t configured correctly.