Oracle® Cloud

Using the DocuSign Adapter with Oracle Integration 3

F45550-05
April 2024

Oracle Cloud Using the DocuSign Adapter with Oracle Integration 3,

F45550-05

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 DocuSign Adapter

Review the following conceptual topics to learn about the DocuSign 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.

DocuSign Adapter Capabilities

To integrate your applications with DocuSign, add the DocuSign Adapter as an integration in Oracle Integration.

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. Key features of DocuSign Adapter include:

- Specified signer routing order for multiple signers
- Delegation of signing responsibility to others

The DocuSign Adapter is one of many predefined adapters included with Oracle Integration. You can configure the DocuSign Adapter as a target 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 DocuSign Adapter Use Cases

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

- Select the **Send an envelope or create a draft** in one integration to create an envelope and send it to recipients or save it as a draft. Select and configure the REST Adapter as

the source. Appropriate data mapping between the REST Adapter and DocuSign Adapter is performed in the mapper. Invoke the integration endpoint with a REST client to send a POST request to the REST Adapter. The DocuSign Adapter sends the data as a payload while invoking the configured operation in DocuSign.

- Select the **Get envelope status changes** operation in one integration to return envelope status changes for all envelopes. Appropriate data mapping between the REST Adapter and DocuSign Adapter is performed in the mapper. The REST Adapter sends a GET request to the DocuSign Adapter , which returns status change information for all envelopes.

Workflow to Create and Add a DocuSign 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.

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

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 DocuSign Adapter Connection
2	Create the integration. When you do this, you add source and target connections to the integration.	Understand Integration Creation and Best Practices in *Using Integrations in Oracle Integration 3* and Add the DocuSign Adapter Connection to an Integration
3	Map data between the source connection data structure and the target 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 DocuSign 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

A DocuSign integrator key (client ID) and client secret are required to create a DocuSign Adapter connection. A DocuSign integrator key is a unique identifier for each DocuSign integration and is used to authenticate your API calls with DocuSign. To move your integration to DocuSign production, you must be certified and get your integrator key authorized by DocuSign.

> **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`. To upload the certificate, see Upload a Certificate to Connect with External Services.
> - The DocuSign Adapter does *not* use the connectivity agent to communicate with DocuSign.

1. Log in to your DocuSign developer account at https://appdemo.docusign.com/home.
   a. If you do not have an account, create one here: https://www.docusign.com/developer-center#form-devaccount.
   b. Follow the steps to create and activate the account.
   c. Create a sandbox.
2. Click **Settings** in the title bar.
3. In the left navigation menu, scroll to **INTEGRATIONS**, and click **Apps and Keys**.
4. On the Apps and Keys page, click **ADD APP AND INTEGRATION KEY**.
5. In the Add Integration Key dialog, enter a name for the app in the **App Name** field, and click **CREATE APP**.
6. On your app's page under **General Info**, note the **Integration Key**.

7. Click the **Copy to clipboard** icon to copy the integration key value.
8. In the **Authentication** section:
   a. Under **User Application**, select **Authorization Code Grant**.
   b. Under **Secret Keys**, click **ADD SECRET KEY**.
   c. Click the **Copy to clipboard** icon to copy the secret key value.
   d. Note the secret key value. You'll require it while configuring the integration key on the Connections page.
9. In the **Additional settings** section under **Redirect URIs**, click **ADD URI** and enter your redirect URI.

> **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`

10. Click **Apps and Keys** to go back to the Apps and Keys page. The newly created app is displayed under **Apps and Integration Keys**.
11. Get the **API Account ID**.
    If you need to log in to multiple accounts for a given login user, get the API account ID.
    a. Under **My Account Information** on the Apps and Keys page, copy the **API Account ID**.
    b. Click the **Copy to clipboard** icon.

c. Note the value of the **API Account ID**. You specify this value when configuring the account ID on the Connections page.

12. Get the DocuSign **Account ID**.
    a. Click the profile image on the upper-right side of the page.
    b. On the menu that displays, note the Account ID that is under the name or organization name. You specify this value before the API Account ID when configuring the account ID on the Connections page.

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

Use this procedure to define the security settings for your DocuSign Adapter connection.

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

   The DocuSign Adapter supports the DocuSign OAuth Authorization Code Credentials security policy by default.

2. Enter the following details.

Element	Description
Client ID (Integrator Key)	Enter the DocuSign integrator key. The key identifies the client (the software requesting an access token) making the request. The value passed in this parameter must exactly match the value shown in the **API and Keys** section of your application in DocuSign. See Prerequisites for Creating a Connection.
Client Secret	Enter the client secret. The client secret authorizes the client (the software requesting an access token) making the request. This value must exactly match the value in the **API and Keys** section of your application in DocuSign. See Prerequisites for Creating a Connection.
Confirm Client Secret	Enter the client secret a second time.

Element	Description
Scope	Enter the space-delimited set of scopes to which you consented (for example, `signature extended`).
Instance Type	Select either **Production** or **Sandbox**. This is an optional field.
Account ID	Enter the account ID. This ID enables you to log into multiple accounts for a given login user. Obtain the value from the **API and Keys** section of your application in DocuSign. See Prerequisites for Creating a Connection. This is an optional field.

3. Click **Provide Consent**.
4. Log in as the user for the instance type that you selected in step 2.

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**.

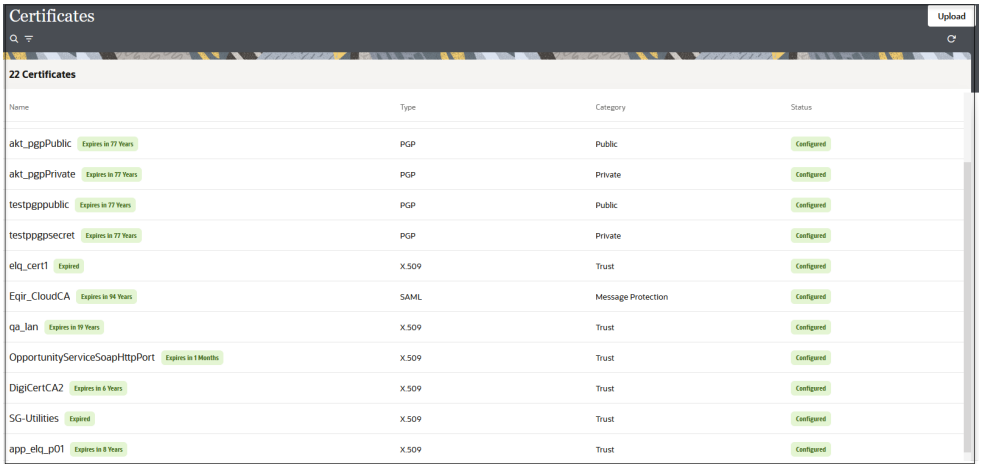
Upload a Certificate to Connect with External Services

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 DocuSign Adapter Connection to an Integration

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

These topics describe the wizard pages that guide you through configuration of the DocuSign Adapter as an invoke in an integration. The DocuSign 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 DocuSign Adapter invoke operation values for your integration.

The table provides definitions for the DocuSign Adapter API operations that can be performed on the target. These operations are listed on the DocuSign Adapter Operations page.

Operation	Description
Send an envelope or create a draft	Creates an envelope and sends it to recipients or saves it as a draft envelope.
Send an envelope from a template	Creates an envelope from an existing template and sends it or saves it as a draft envelope.
Retrieving envelope and documents	When the envelope status is `completed`, returns the signed document and associated certificate from the server.
Get envelope status changes	Returns envelope status changes for all envelopes.
Get individual envelope status	Returns the overall status for a single envelope.
Send draft envelope	Sends a single draft envelope.
Void envelope	Voids a single in-process envelope.
Modify draft envelope email subject and message for draft envelope	Modifies the email subject and message of draft envelopes.
Purge documents	Places envelope documents and metadata in a purge queue so they can be removed from DocuSign.

Element	Description
Select Operation	Select the API operation to perform.

Invoke Request Page

Enter the DocuSign Adapter request parameters.

You can configure the request query parameters on the DocuSign 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 following table are available for the operation `Get envelope status changes`.

Parameter	Description
`transactionIds`	Returns a comma separated list of envelope transactionIds when included in the query string. Returns a list of envelope transactionIds when included in the request_body. transactionIds are only valid in the DocuSign system for seven days.
`status`	The list of current statuses to include in the response. By default, all envelopes found are returned. If values are specified, then of the envelopes found, only those with the current status specified are returned in the results.
`from_to_status`	The status type checked for in the from_date/to_date period. If `changed` is specified, then envelopes that changed status during the period are returned. If `created` is specified, then envelopes created during the period are found. The default is `changed`.
`envelopeId`	Specifies the envelope ID.
`ac_status`	Specifies the authoritative copy status for envelopes.
`to_date`	Returns items up to the specified date. If a value is not provided, the default search is to the current date.

Parameter	Description
`custom_field`	Specifies the envelope custom field name and value searched for in the envelope information.
`from_date`	Returns items on or after the specified date. If a value is not provided, the default search is the previous 30 days.

Element	Description
Query Parameters	Filters the query parameters by name.
Available Query Parameters	Lists the available query parameters for the selected API operation.
Selected Query Parameters	Lists the selected query parameters for the selected API operation.

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**.