

Oracle® Construction and Engineering Using the Aconex Adapter with Oracle Integration 3



F89912-02
June 2024



Oracle Construction and Engineering Using the Aconex Adapter with Oracle Integration 3,
F89912-02

Copyright © 1999, 2024, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

Contents

Preface

Audience	iv
Documentation Accessibility	iv
Diversity and Inclusion	iv
Related Resources	v
Conventions	v

1 Understand the Aconex Adapter

Aconex Adapter Capabilities	1-1
Aconex Adapter Restrictions	1-2
Aconex Adapter Use Cases	1-2
What Application Version Is Supported?	1-3
Workflow to Create and Add a Connection to an Integration	1-3

2 Create an Aconex Adapter Connection

Prerequisites for Creating a Connection	2-1
Create a Connection	2-2
Configure Connection Properties	2-3
Configure Connection Security	2-3
Test the Connection	2-3
Upload a Certificate to Connect with External Services	2-4

3 Add the Aconex Adapter Connection to an Integration

Basic Info Page	3-1
Configure Operations Page	3-1
Summary Page	3-2

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 the Aconex Adapter 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](#)
- [Aconex Help Documentation](#)

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.
<i>italic</i>	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 Aconex Adapter

Review the following topics to learn about the Aconex 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:

- [Aconex Adapter Capabilities](#)
- [Aconex Adapter Restrictions](#)
- [What Application Version Is Supported?](#)
- [Workflow to Create and Add a Connection to an Integration](#)

Aconex Adapter Capabilities

The Aconex Adapter enables you to set up a connection with Aconex. It is one of many predefined adapters included with Oracle Integration. You can configure the Aconex Adapter as an invoke connection within an integration in Oracle Integration.

Adapter Capabilities

- **Easy API Module Selection** : Facilitates the seamless selection of various Aconex API modules, including:
 - Directory
 - Documents
 - Mail
 - Project Fields
 - Projects Tasks
 - User Roles
 - Workflows
- **Simple Operation Selection**: Allows effortless selection of specific operations (API service endpoints) within each selected API module. Each operation is accompanied by a basic description for usage clarification.
- **Intuitive Data Mapping Functionality**: Supports intuitive data mapping based on the selected operation, with mandatory fields highlighted as necessary.
- **Automatic Population of Request Parameters**: Automatically populates common request parameters essential for a successful API request, streamlining the integration process.

Adapter Benefits

- **Accelerated Integration Timeline**: Significantly reduces the time required to create integrations with Aconex through Oracle Integration.
- **Simplified Integration Process**: Enables seamless integration of Aconex with other applications, even without extensive knowledge of Oracle Integration or Aconex REST

APIs. While familiarity with REST APIs can enhance certain functionalities, it is not mandatory for basic integration tasks.

- **No Dependency on the Generic REST Adapter:** Eliminates the need to rely on a generic REST adapter, providing a tailored solution for Aconex integration needs.

Aconex Adapter Restrictions

The Aconex Adapter has the following restrictions:

- **Single File Synchronization:** Supports synchronizing only one file at a time, including file uploading and editing within the Documents and Mails modules.
- **Optimized for Small File Uploads:** Does not support the *Large File Upload* approach within the Documents module, particularly for Register Document and Supersede Document API operations. The *Small File Upload* method is recommended for files up to 100 MB.
- **Basic Authentication Support:** Only supports Basic Authentication (Basic Auth). Advanced authentication mechanisms (such as OAuth) are not supported yet.



Note:

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

Aconex Adapter Use Cases

The Aconex Adapter streamlines integration between Aconex and other applications. It provides comprehensive capabilities across various API modules and ensures efficient and accurate synchronization of critical project data.

The Aconex Adapter can be used in the following scenarios:

- **Document Management:** The adapter facilitates the integration flows for uploading documents to Aconex. It automates the upload process to ensure all necessary documents, including metadata and required fields are available in Aconex. It also supports keeping the documents current by using the adapter suppression and update operations. Additionally, the adapter provides the ability to interrogate the information of a document, which is critical for reporting.
- **Mail Management:** The adapter automates mail operations, such as creating, replying, and viewing of mail content and metadata based on actions in your source application. This automation streamlines communication and ensures that the important project information is appropriately addressed. Additionally, the adapter can integrate mail attachment downloads into the target application workflow, ensuring all relevant attachments are saved and accessible. This enhances information availability and improves project documentation. The adapter also facilitates the viewing and management of mail metadata and schemas, keeping mail-related information organized and easily accessible.
- **Project Management:** The adapter automates the process of inviting users to projects in Aconex, based on changes in the source application, ensuring efficient and accurate user management across your project teams.

- **Project Fields Management:** The adapter automates creation, editing, enabling, and disabling of project fields in Aconex. This ensures that all necessary project fields are accurately maintained and updated in line with the source application project requirements.
- **Task Management:** The adapter integrates tasks from Aconex into the primary project management tool, keeping all task-related information synchronized.
- **User Role Management:** The adapter can be used for updating user roles across systems by synchronizing role assignments. This helps maintain correct user permissions and access levels across various project management tools. Additionally, it can automate the process of managing user roles within Aconex based on changes in the source application, ensuring efficient and accurate user management across the project teams.
- **Workflow Integration:** The adapter can create integration flows that track workflow status changes in Aconex, keeping the target project management tool updated with the latest status and ensuring better tracking and management of project workflows.

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 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	Access Oracle Integration.	Go to <code>https://instance_URL/ic/home</code>
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 an Aconex Adapter Connection
3	Create the integration. When you do this, you add trigger (source) and invoke (target) connections to the integration.	Create Integrations in <i>Using Integrations in Oracle Integration 3</i> and Add the Aconex Adapter Connection to an Integration
4	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in <i>Using Integrations in Oracle Integration 3</i>
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 <i>Using Integrations in Oracle Integration 3</i>
6	Activate the integration.	Activate an Integration in <i>Using Integrations in Oracle Integration 3</i>
7	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in <i>Using Integrations in Oracle Integration 3</i>

Step	Description	More Information
8	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Track Integration Instances in <i>Using Integrations in Oracle Integration 3</i>
9	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in <i>Using Integrations in Oracle Integration 3</i>

2

Create an Aconex 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

Every integration with Aconex APIs must be registered with Oracle using Basic Authentication. You will receive the credentials required to uniquely identify the integration.

Oracle Aconex Customers

Oracle Aconex customers have two options for testing their integrations before enabling them in production on their live projects:

- **Early Access Environment:** Oracle provides an Early Access (EA) environment for testing Smart Construction Platform integrations in a non-production environment.
- **Training and Practice Project:** Every Aconex instance has a Training and Practice project available for you to use. Your Oracle contact can arrange an invitation to it upon request.

For the **EA approach**, your integration journey would be:

1. Register your organization in the EA environment.
2. Create test users and test data in EA.
3. [Register your integration](#) in EA.
4. Complete your integration testing in EA.
5. Register your integration in production.
6. Go live in production by deploying a separate production version.

For the **Training and Practice** approach, your integration journey would be:

1. Register your integration in production.
2. Request access to the Training and Practice project.
3. Complete your integration testing using the Training and Practice project.
4. Go live by connecting to your live projects.

Oracle Technology Partners

Oracle Technology Partners must join the Oracle Partner Network (OPN) and complete their testing in the EA environment before publishing to production. Your published integration will be available to all users.

Oracle Technology Partners' integration journey looks like this:

1. Join the [Oracle PartnerNetwork](#) (OPN).
2. Register your organization on the EA environment.
3. Create test users and test data in EA.
4. Register an integration in EA.
5. Complete your integration testing in EA.
6. Publish your integration to production.

For more information, refer to the [Getting started with APIs](#) topic in the Aconex [REST API documentation](#).

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.
 - a. Enter a meaningful name to help others find your connection when they begin to create their own integrations. The name you enter is automatically added in capital letters to the **Identifier** field. If you modify the identifier name, don't include blank spaces (for example, SALES OPPORTUNITY).
 - b. 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.
 - c. Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
 - d. Enter an optional description of the connection.
5. Click **Create**.

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

Configure Connection Properties

Enter connection information so your application can process requests.

1. Go to the **Properties** section.
2. In the **Connection URL** field, specify the URL of your Aconex instance.
3. From the **Connection Type** list, select **REST API Base URL**.

Configure Connection Security

Configure security for your Aconex Adapter connection.

1. Go to the **Security** section.
2. In the **User Name** field, enter the Aconex integration user account username.
3. In the **Password** field, enter the Aconex integration user account password.

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: <ul style="list-style-type: none"> • 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 *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 Aconex Adapter Connection to an Integration

When you select and place the Aconex Adapter into the invoke area of an integration, the Adapter Endpoint Configuration Wizard is invoked. This wizard guides you through configuration of the Aconex Adapter endpoint properties.

The following topics describe the wizard pages that guide you through configuration of the Aconex Adapter as an invoke in an integration.

Topics:

- [Basic Info Page](#)
- [Configure Operations Page](#)
- [Summary Page](#)

Basic Info Page

You can enter the endpoint name, functionality, and select an API module on the Basic Info page.

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: <ul style="list-style-type: none">• 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 for the connection's functionality. For example: <code>This endpoint executes a search of an organization's document register for a project.</code>
Select an API module	Select a specific Aconex service API module from the list of available options.

Configure Operations Page

Specify the operation that you want your selected API module to perform.

Element	Description
Select Operation	Each API module offers specific operations that you can perform. Choose an operation based on the your selected module.

Element	Description
Operation Description	Briefly describe the selected operation's functionality.

Summary Page

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

Element	Description
Summary	<p>Displays a summary of the configuration values you defined on previous pages of the wizard.</p> <p>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.</p> <p>To return to a previous page to update any values, click the appropriate tab in the left panel or click Back.</p> <p>To cancel your configuration details, click Cancel.</p>
