Oracle® Cloud

Using the RosettaNet Adapter with Oracle Integration 3

F89713-03

April 2024

Oracle Cloud Using the RosettaNet Adapter with Oracle Integration 3,

F89713-03

Primary Author: Oracle Corporation

Contents

Preface

1 Understand the RosettaNet Adapter

2 Create a RosettaNet Adapter Connection

3 Add the RosettaNet Adapter Connection to an Integration

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 RosettaNet Adapter

Review the following topics to learn about the RosettaNet 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:

- RosettaNet Adapter Capabilities
- RosettaNet Adapter Restrictions
- What Application Version Is Supported?

RosettaNet Adapter Capabilities

The RosettaNet Adapter enables you to create an integration between a RosettaNet trading partner and Oracle Integration. The RosettaNet standard defines both e-commerce document and exchange protocols as part of the Electronic data interchange (EDI). The RosettaNet standard is XML-based, and defines message guidelines, interfaces for business processes, and implementation frameworks for interactions between trading partners.

The RosettaNet Adapter provides the following capabilities:

- Support for trigger and invoke connections for receiving inbound messages from a trading partner and sending outbound messages to a trading partner.
- Support for RosettaNet Implementation Framework (RNIF) 2.0 protocol features:
  - Partner interface processes (PIPs)
  - RosettaNet business message handling
  - Multipurpose Internet Mail Extension (MIME) headers
  - Encryption
  - Signature over HTTPS
- Support for defining RosettaNet schemas and attaching documents to trading partner setups for processing through B2B for Oracle Integration. See B2B Documents and B2B Schemas in *Using B2B for Oracle Integration 3*.

See About RosettaNet in *Using B2B for Oracle Integration 3*.

The RosettaNet Adapter is one of many predefined adapters included with Oracle Integration. You can configure the RosettaNet Adapter as a trigger and an invoke connection in an integration in Oracle Integration.

RosettaNet Adapter Restrictions

Note the following RosettaNet Adapter restrictions.

- The Message Disposition Notification (MDN) is not supported.

- The RosettaNet Adapter only works in B2B trading partner mode. B2B standalone mode is not supported.

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

What Application Version Is Supported?

For information about which application version is supported by this adapter, see the Connectivity Certification Matrix.

2

Create a RosettaNet 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

Satisfy the following prerequisites specific to your environment to create a connection with the RosettaNet Adapter.

This information is required to create a RosettaNet Adapter connection on the Connections page. See Configure Connection Properties and Configure Connection Security.

- Trading Partner Endpoint Prerequisites
- Certificate and Private Key Prerequisites
- RosettaNet Advanced Policy Prerequisites
- RosettaNet Basic Policy Prerequisites
- Two-Way SSL Connections in the Outbound Direction Prerequisites

Trading Partner Endpoint Prerequisites

- Ensure that the trading partner's RosettaNet endpoint to use is reachable from Oracle Integration.
- Know the URL of the trading partner endpoint at which to receive RosettaNet messages.

Certificate and Private Key Prerequisites

Ensure that the necessary certificates and private keys used for encryption, decryption, signature generation, and signature verification are uploaded. See Upload a Certificate to Connect with External Services.

RosettaNet Advanced Policy Prerequisites

To use the RosettaNet Advanced Policy, know the following information based on what you plan to configure on the Connections page:

- RosettaNet decryption private key alias and key password
- Inbound RosettaNet sign verify certificate alias
- RosettaNet endpoint username and password
- RosettaNet signature private key alias and password

- Outbound RosettaNet encrypt certificate alias

RosettaNet Basic Policy Prerequisites

To use the RosettaNet Basic Policy, know the following information based on what you plan to configure on the Connections page:

- HTTP authentication username and password
- Private key alias and password
- Partner certificate alias

Two-Way SSL Connections in the Outbound Direction Prerequisites

If you want to use two-way SSL connections in the outbound direction, perform the following steps.

> **Note:**
>
> Two-way SSL connections in the inbound (trigger) direction are not supported.

1. Generate a client certificate. The tasks are similar to what you perform for the REST Adapter or SOAP Adapter, except that the transport layer security (TLS) version is not needed. For an overview, see Create a Keystore File for a Two-Way, SSL-Based Integration in *Using the REST Adapter with Oracle Integration 3*.
2. Upload the certificate as an X.509 Identity. See Upload a Certificate to Connect with External Services.
3. Remember the key alias you use.
4. Configure a two-way SSL connection. See Configure Connection Properties. The settings you configure on the Connections page are used at runtime by the RosettaNet Adapter to perform SSL client authentication for a RosettaNet inbound business message.

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.
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 Properties

Enter connection information so your application can process requests. This section only appears when you configure the RosettaNet Adapter as an invoke connection.

1. Go to the **Properties** section.
2. In the **RosettaNet Service URL** field, enter the endpoint address of the trading partner to receive RosettaNet messages.
3. Expand **Optional properties**.

Element	Description
Enable two way SSL for outbound connections	Select **Yes** if you want to enable communication.
Client Identity Key Alias (Two Way SSL)	Enter the certificate key alias to use for client identity during two-way SSL communication.

Configure Connection Security

Configure security for your RosettaNet Adapter connection.

1. Go to the **Security** section.
2. Select the security policy to use.
   a. If you select **RosettaNet Basic Policy**, and expand **Optional security**.

Element	Description
Username	Enter the username to use for HTTP authentication of the partner's protected endpoint address.
Password	Enter the password to use for HTTP authentication of the partner's protected endpoint address.
Private Key Alias	Enter the private key used for inbound data decryption and outbound signature generation. This is the same key alias as uploaded in the identity store when you select **Settings** and then **Certificates** in the navigation pane.
Key Password	Enter the password associated with the private key.
Partner Certificate Alias	Enter the partner certificate to use for outbound data encryption and inbound signature verification.

   b. If you select **RosettaNet Advanced Policy**, and expand **Optional security**.

Element	Description
Private Key Alias (RosettaNet Decryption)	Enter the private key used for inbound data decryption by a trigger action.

Element	Description
Key Password (RosettaNet Decryption)	Enter the key password associated with the private key.
Certificate Alias (Inbound RosettaNet Sign Verify)	Enter the partner public key certificate used by a trigger connection for inbound RosettaNet certificate verification.
Username (RosettaNet Endpoint)	Enter the user name required for sending the RosettaNet password to the protected partner endpoint.
Password (RosettaNet Endpoint)	Enter the password required for sending the RosettaNet password to the protected partner endpoint.
Private Key Alias (RosettaNet Signature)	Enter the private key used by the invoke connection to send a signed RosettaNet message.
Key Password (RosettaNet Signature)	Enter the key password associated with the private key (RosettaNet signature).
Certificate Alias (Outbound RosettaNet Encrypt)	Enter the partner public certificate used by an invoke connection for outbound RosettaNet message encryption. This is the same key alias as uploaded in the identity store when you select **Settings** and then **Certificates** in the navigation pane.

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.

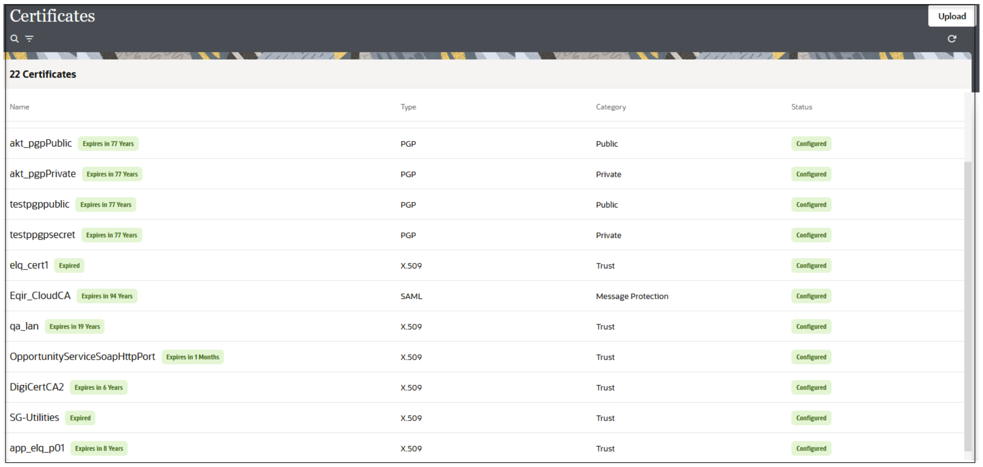
2. Wait for a message about the results of the connection test.
   - If the test was successful, then the connection is configured properly.
   - If the test failed, then edit the configuration details you entered. Check for typos and verify URLs and credentials. Continue to test until the connection 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.
      1. Click **Browse**, then select the PGP file to upload.
      2. 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.
      3. 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 RosettaNet Adapter Connection to an Integration

You select the RosettaNet Adapter as a trigger (receive) or invoke (send) connection when configuring the RosettaNet transport. The RosettaNet Adapter works in B2B trading partner mode and uses B2B trading partner profiles. You configure those settings by selecting **B2B**, then **Trading Partners** in the navigation pane.

Topics:

- Basic Info Page
- Summary Page

See Create B2B Integrations for Receiving and Sending and Define a RosettaNet Transport in *Using B2B for Oracle Integration 3*.

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.`

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**.