Oracle® Cloud

Using the AS4 Adapter with Oracle Integration 3

G16460-05
June 2025

Oracle Cloud Using the AS4 Adapter with Oracle Integration 3,

G16460-05

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 AS4 Adapter

Review the following topics to learn about the AS4 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:

AS4 Adapter Capabilities

The AS4 Adapter enables you to create an integration between an AS4 trading partner and Oracle Integration. Applicability Statement 4 (AS4) is a protocol for transporting structured business-to-business (B2B) data securely and reliably over the internet. Security is achieved by using digital certificates, encryption, and message compression.

The AS4 Adapter provides the following capabilities:

- Supports trigger and invoke connections for handling inbound and outbound AS4 messages.
- Supports encryption/decryption, signing/signature verification, and compression/decompression of messages as per AS4 specifications.
- Supports the following payload types: EDI, XML, or anything that AS4 can support.
- Establishes a connection to the AS4-compliant B2B system to enable sending or receiving messages.
- Supports synchronous, unsigned MDN.
- Enables you to configure outbound and inbound message delivery using the Adapter Endpoint Configuration Wizard.
- Consumes business messages and MDN acknowledgments in the inbound direction. Synchronous MDN acknowledgment deliveries are supported.
- Supports the AS4 Basic Username Password Token Policy and AS4 Advanced Username Password Token Policy security policies.
- Supports specifying the message partition channel (MPC) value on which the inbound or outbound AS4 message is set. See Specify the Message Partition Channel Value for the Inbound or Outbound AS4 Message.

The AS4 Adapter is one of many predefined adapters included with Oracle Integration. See the Adapters page in the Oracle Help Center.

AS4 Adapter Restrictions

Note the following AS4 Adapter restrictions.

- When uploading an SSL certificate, select only the X.509 (SSL transport) type. The AS4 Adapter does not support selecting the SAML (Authentication & Authorization), PGP (Encryption & Decryption), or Signing key type. See Upload a Certificate to Connect with External Services.
- Asynchronous MDN is not supported.
- Signed MDN is not supported.
- Signed/encrypted AS4 messages only have an inline payload (that is, within the SOAP body). These messages do not contain a compressed payload or a payload as an attachment.
- The AS4 Adapter cannot be used in standalone mode.
- Connectivity to an on-premises B2B system through the connectivity agent is not supported.
- Persistence of messages by the AS4 Adapter is not supported. Instead, design persistence in the overall 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.

What Application Version Is Supported?

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

2

Create an AS4 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

You must satisfy the following prerequisites to create a connection with the AS4 Adapter:

This information is required to create an AS4 Adapter connection on the Connections page. See Configure Connection Properties and Configure Connection Security.

Trading Partner Endpoint Prerequisites

- Ensure that the trading partner's AS4 endpoint to use is reachable from Oracle Integration.
- Know the URL of the trading partner endpoint at which to receive AS4 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.

AS4 Advanced Username Password Token Policy Prerequisites

To use the AS4 Advanced Username Password Token Policy, know the following information based on what you plan to configure on the Connections page:

- Inbound AS4 sign verify certificate alias
- AS4 decryption private key alias and key password
- AS4 endpoint user name and password
- AS4 signature private key alias and password
- Outbound AS4 encrypt certificate alias
- Asynchronous receipt authentication user name and password

- Private key and password to deliver a signed receipt
- Inbound receipt signature verification certificate
- Outbound response receipt verification certificate

AS4 Basic Username Password Token Policy Prerequisites

To use the AS4 Basic Username Password Token Policy, know the following information based on what you plan to configure on the Connections page:

- HTTP authentication user name 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 AS2 Adapter to perform SSL client authentication for two types of outgoing messages:
   - An AS4 outbound business message.
   - An outgoing asynchronous MDN message sent in response to an inbound AS4 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.

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

To create a connection in Oracle Integration:

1. Decide where to start:
   - Work in a project (see why working with projects is preferred).
     a. In the navigation pane, click **Projects**.
     b. Select the project name.
     c. Click **Integrations**.
     d. In the **Connections** section, click **Add** if no connections currently exist or **+** if connections already exist. The Create connection panel opens.
   - Work outside a project.
     a. In the navigation pane, click **Design**, then **Connections**.
     b. Click **Create**. The Create connection panel opens.
2. 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.
3. 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. **Note**: *Only* the roles supported by the adapter you selected are displayed for selection. Some adapters support all role combinations (trigger, invoke, or trigger and invoke). Other adapters support fewer role combinations. 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.

Element	Description
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.

4. Click **Create**.

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

5. Follow the steps to configure a connection.
   The connection property and connection security values are specific to each adapter. Your connection may also require configuration with an access type such as a private endpoint or an agent group.

6. Test the connection.

Configure Connection Properties

Enter connection information so your application can process requests.

1. Go to the **Properties** section.
2. In the **AS4 service URL** field, specify the URL of the trading partner endpoint at which AS4 messages are received.

   This field is only displayed when configuring the AS4 Adapter as an invoke connection. There are no connection properties required when configuring the AS4 Adapter as a trigger connection.

3. If you selected the **Invoke** or **Trigger and invoke** role, optionally select to use two-way SSL connections in the outbound direction. This feature is not available if you select the **Trigger** role. Ensure that you have first completed all two-way SSL connection prerequisites. See Prerequisites for Creating a Connection.

   > **Note:**
   >
   > If you need to use both asynchronous message disposition notifications (MDNs) and two-way SSL, ensure that you selected the **Trigger and invoke** role when creating the AS4 Adapter connection.

   a. From the **Enable two-way SSL for outbound connections** list, select **Yes** if you want to enable two-way SSL for outbound connections. Otherwise, select **No**.

   b. In the **Client identity key alias (two way SSL)** field, enter the certificate alias to use to establish client identity during two-way SSL communication.

If the test connection fails because two-way SSL communication didn't happen correctly, note that different servers may respond differently. See Troubleshoot Two-Way SSL Connections.

Configure Connection Security

Configure security for your AS4 Adapter connection.

1. Go to the **Security** section.
2. Select the security policy and enter the associated credentials.

> **Note:**
>
> - All credential fields are optional by default. However, they are required for achieving various levels of message security. See the Comments column in the tables below.
> - Import the partner certificates and private keys described in this section on the Certificates page available by selecting **Settings**, and then **Certificates**. Upload of only the **X.509 (SSL transport)** type is supported. See Upload a Certificate to Connect with External Services.

a. If you select **AS4 Advanced Username Password Token Policy**:

This security policy provides finer control and flexibility for using separate certificates and keys for different operations (for example, encrypt, decrypt, sign, and sign verify). This security policy enables you to specify separate user names and passwords for AS4 authentication.

Login Credentials	Comments
• **Username (Async Receipt)**: Enter the user name used by a trigger connection for authentication while sending an outbound receipt. • **Password (Async Receipt)**: Enter the password used by a trigger connection for authentication while sending an outbound receipt.	These are optional fields, but are required for authentication while sending an outbound receipt.
• **Private Key Alias (AS4 Decryption)**: Enter the private key alias used by a trigger connection for inbound data decryption. This is the same key that you upload for the **Identity** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**. • **Key Password (AS4 Decryption)**: Enter the password for the private key used by a trigger connection for inbound data decryption.	These are optional fields, but are required for inbound data decryption of business messages.

Login Credentials	Comments
• **Private Key Alias (Receipt Signature)**: Enter the private key used by a trigger connection to deliver a signed receipt. This is the same key that you upload for the **Identity** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**. • **Key Password (Receipt Signature)**: Enter the password associated with the private key to deliver a signed receipt.	These are optional fields, but are required for inbound signed receipt delivery of business messages.
• **Certificate Alias (Inbound AS4 Sign Verify)**: Enter the partner public certificate used by a trigger connection for inbound AS4 signature verification. This is the same certificate that you upload for the **Trust** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**.	This is an optional field, but is required for inbound signature verification of business messages.
• **Certificate Alias (Inbound Receipt Sign Verify)**: Enter the partner public certificate used by a trigger connection for inbound receipt signature verification. This is the same certificate that you upload for the **Trust** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**.	This is an optional field, but is required for inbound receipt signature verification of business messages.
• **Username (AS4 endpoint)**: Enter the username used by an invoke connection for sending an AS4 message to a protected partner endpoint. • **Password (AS4 endpoint)**: Enter the password required for sending the AS4 message to the protected partner endpoint.	These are optional fields, but are required for sending business messages to a partner's secured endpoint.
• **Private key alias (AS4 signature)**: Enter the private key used by an invoke connection to send a signed AS4 message. This is the same key that you upload for the **Identity** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**. • **Key password (AS4 signature)**: Enter the password associated with the private key (AS4 signature) uploaded on the Certificates page by selecting **Settings**, and then **Certificates**.	These are optional fields, but are required for outbound signature generation of business messages.
• **Certificate Alias (Outbound AS4 Encrypt)**: Enter the partner public certificate used by an invoke action for outbound AS4 message encryption. This is the same certificate that you upload for the **Trust** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**.	This is an optional field, but is required for outbound data encryption of business messages.

Login Credentials	Comments
• **Certificate Alias (Response Receipt Sign Verify)**: Enter the partner public certificate used by an invoke action for outbound response receipt certificate verification. This is the same certificate that you upload for the **Trust** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**.	This is an optional field, but is required for outbound response receipt certificate verification.

b. If you select **AS4 Basic Username Password Token Policy**.

This security policy requires you to specify minimal configuration details to work in an integration.

Login Credentials	Comments
• **Username**: Enter the username used for HTTP authentication of the trading partner's protected endpoint. • **Password**: Enter the password used for HTTP authentication.	These are optional fields, but are required for sending business messages and asynchronous MDN acknowledgments to a partner's secured endpoint.
• **Private key alias**: Enter the private key used for inbound data decryption and outbound signature generation. This is the same key that you upload for the **Identity** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**. • **Key password**: Enter the password associated with the private key that you upload on the Certificates page by selecting **Settings**, and then **Certificates**.	These are optional fields, but are required for inbound data decryption of business messages and outbound signature generation for business messages and MDN acknowledgments.
• **Partner certificate alias**: Enter the partner certificate used for outbound data encryption and inbound signature verification. This is the same key that you upload for the **Trust** category of the **X.509 (SSL transport)** type by selecting **Settings**, and then **Certificates**.	This is an optional field, but is required for outbound data encryption of business messages, signature verification of synchronous MDN responses in adapter invoke operations, and inbound signature verification of business messages and MDN acknowledgments.

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.

If Your Connection...	Then...
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.

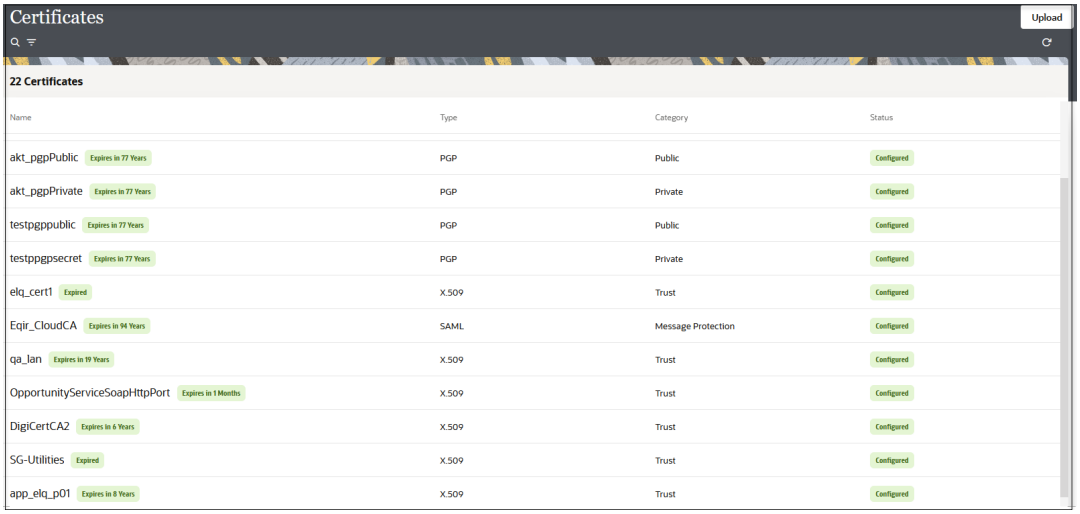
2. Wait for a message about the results of the connection test.
   - If the test was successful, then the connection is configured properly.
   - If the test failed, then edit the configuration details you entered. Check for typos and verify URLs and credentials. Continue to test until the connection 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 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 AS4 Adapter Connection to an Integration

The AS4 Adapter works only in B2B trading partner mode, and not standalone mode. The Adapter Endpoint Configuration Wizard only includes configuration pages for the name and description of the endpoint. AS4 Adapter configuration is only used in integrations as part of the autogenerated transports.

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.`

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

Implement Common Patterns Using the AS4 Adapter

You can use the AS4 Adapter to implement the following common pattern.

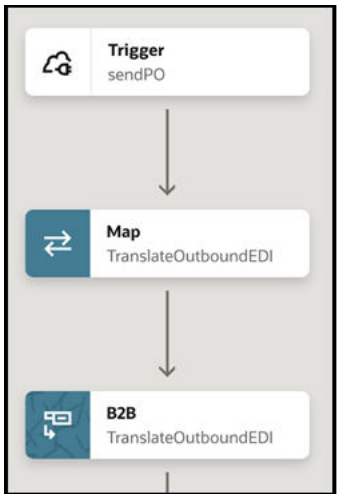
Topics:

Specify the Message Partition Channel Value for the Inbound or Outbound AS4 Message

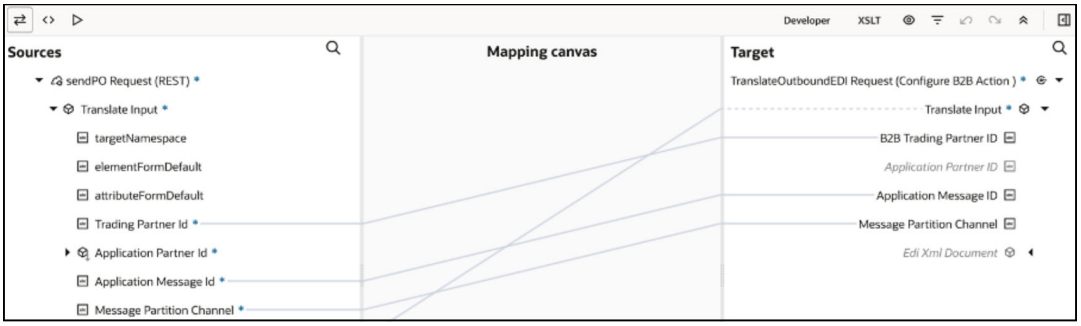
You can specify the message partition channel (MPC) value with the **Message Partition Channel** element in the mapper for the inbound pull or outbound push of an AS4 message.

MPCs allow for the partitioned transfer of AS4 messages between AS4 exchange participants. MPCs are used for both pushed and pulled messages. One MPC is used for a single message exchange between two participants. You use the **Message Partition Channel** element in the mapper to specify the MPC value on which the inbound or outbound AS4 message is set. That message is eventually pulled upon receiving the inbound pull request or pushed upon sending the outbound push response as per the AS4 specification.

1. Open the integration in which to specify the MPC value. For this example, an inbound pull is demonstrated.



2. Open the mapper.
3. Map the **Message Partition Channel** source element to the **Message Partition Channel** target element under **TranslateOutboundEDI Request**.



4. Save your changes.

5

Troubleshoot the AS4 Adapter

Review the following topic to learn about troubleshooting issues with the AS4 Adapter.

Topics:

Troubleshoot Two-Way SSL Connections

If the test connection fails because two-way SSL communication didn't happen correctly, note that different servers may respond differently. The following two different behaviors are identified, but there can be other variations. When you test the connection on the Connections page, both of these cases are reported as failures.

- If a proper client certificate wasn't presented by the AS4 Adapter, the remote server can close the TCP connection unilaterally. On the client side, no response is received. The server instead closes the connection abruptly.
- A remote server may send a response with an HTTP status code such as `400` (bad request) or `403` (forbidden). The server may or may not include the reason in the response.