Oracle® Cloud

Using the AS2 Adapter with Oracle Integration Generation 2

F29723-08
December 2022

Oracle Cloud Using the AS2 Adapter with Oracle Integration Generation 2,

F29723-08

Copyright © 2020, 2022, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

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

1 Understand the AS2 Adapter

AS2 Adapter Capabilities 1-1
AS2 Adapter Restrictions 1-2
What Application Version Is Supported? 1-2
Workflow to Create and Add an AS2 Adapter Connection to an Integration 1-2

2 Create an AS2 Adapter Connection

Prerequisites for Creating a Connection 2-1
Create a Connection 2-2
- Configure Connection Properties 2-3
- Configure Connection Security 2-4
- Test the Connection 2-7

Upload an SSL Certificate 2-7

3 Add the AS2 Adapter Connection to an Integration

Basic Info Page 3-1
Trigger Actions Page 3-2
Trigger Identifiers Page 3-2
Invoke Identifiers Page 3-2
Invoke Headers and Packaging Page 3-3
Invoke MDN Options Page 3-3
Summary Page 3-4

4 Implement Common Patterns Using the AS2 Adapter

Receive an EDI Document from a Trading Partner 4-1
Send an EDI Document to a Trading Partner 4-2
Receive an MDN Acknowledgment from a Trading Partner 4-2

5 Troubleshoot the AS2 Adapter

Troubleshoot Two-Way SSL Connections 5-1

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 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs 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

  `http://cloud.oracle.com`
- *Using Integrations in Oracle Integration Generation 2*
- *Using the Oracle Mapper with Oracle Integration Generation 2*

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 AS2 Adapter

Review the following conceptual topics to learn about the AS2 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:

- AS2 Adapter Capabilities
- AS2 Adapter Restrictions
- What Application Version Is Supported?
- Workflow to Create and Add an AS2 Adapter Connection to an Integration

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

AS2 Adapter Capabilities

The AS2 Adapter enables you to create an integration between an AS2 trading partner and Oracle Integration. Applicability Statement 2 (AS2) 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 AS2 Adapter provides the following benefits:

- Trigger and invoke connections for handling inbound and outbound AS2 messages.
- Encryption/decryption, signing/signature verification, and compression/decompression of messages as per AS2 specifications.
- Supports the following payload types: EDI, XML, or anything that AS2 can support.
- Establishes a connection to the AS2-compliant B2B system to enable sending or receiving messages.
- Supports receiving and sending business messages or MDN acknowledgments.
- Enables you to configure outbound and inbound message delivery using the Adapter Endpoint Configuration Wizard.
- Sends business messages and consumes synchronous MDN acknowledgment in the outbound direction. Produces an encrypted, signed, and compressed business message.
- Consumes business messages and MDN acknowledgments in the inbound direction. Synchronous and asynchronous MDN acknowledgment deliveries are supported.
- Supports basic and advanced security policies. If you select the **Invoke** or **Trigger and Invoke** role when creating an AS2 Adapter connection, you can optionally select to use

two-way SSL connections in the outbound direction. See Configure Connection Properties.

The AS2 Adapter is one of many predefined adapters included with Oracle Integration. You can configure the AS2 Adapter as a trigger or an invoke connection in an integration in Oracle Integration.

See What Is B2B for Oracle Integration in *Using B2B for Oracle Integration Generation 2*.

AS2 Adapter Restrictions

Note the following AS2 Adapter restrictions.

- When uploading an SSL certificate, select only the X.509 (SSL transport) type. The AS2 Adapter does not support selecting the SAML (Authentication & Authorization) or PGP (Encryption & Decryption) type. See Upload an SSL Certificate.
- Connectivity to an on-premises B2B system through the connectivity agent is not supported.
- Persistence of messages by the AS2 Adapter is not supported. Instead, design persistence in the overall integration.

What Application Version Is Supported?

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

See Connectivity Certification Matrix.

Workflow to Create and Add an AS2 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 the adapter tasks and the overall integration tasks, and provides links to instructions for each step.

Step	Description	More Information
1	Access Oracle Integration.	Go to `https://instance_URL/ic/home/`
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 AS2 Adapter Connection
3	Create the integration. When you do this, you add trigger (source) and invoke (target) connections to the integration.	Create Integrations in *Using Integrations in Oracle Integration Generation 2* and Add the AS2 Adapter Connection to an Integration

Step	Description	More Information
4	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in *Using Integrations in Oracle Integration Generation 2*
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 *Using Integrations in Oracle Integration Generation 2*
6	Activate the integration.	Activate Integrations in *Using Integrations in Oracle Integration Generation 2*
7	Monitor the integration on the dashboard.	Monitor Integrations in *Using Integrations in Oracle Integration Generation 2*
8	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Manage Business Identifiers for Tracking Fields in Messages in *Using Integrations in Oracle Integration Generation 2*
9	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in *Using Integrations in Oracle Integration Generation 2*

2

Create an AS2 Adapter Connection

A connection is based on an adapter. You define connections to the specific cloud applications that you want to integrate. The following topics describe how to define connections.

Topics:

- Prerequisites for Creating a Connection
- Create a Connection
- Upload an SSL Certificate

Prerequisites for Creating a Connection

Satisfy the following prerequisites specific to your environment to create a connection with the AS2 Adapter:

This information is required to create an AS2 Adapter connection on the Connections page. See Configure Connection Properties and Configure Connection Security.

- Trading Partner Endpoint Prerequisites
- Certificate and Private Key Prerequisites
- AS2 Advanced Policy Prerequisites
- AS2 Basic Policy Prerequisites
- Two-Way SSL Connections in the Outbound Direction Prerequisites

Trading Partner Endpoint Prerequisites

- Ensure that the trading partner's AS2 endpoint to use is reachable from Oracle Integration.
- Know the URL of the trading partner endpoint at which to receive AS2 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 an SSL Certificate.

AS2 Advanced Policy Prerequisites

To use the AS2 Advanced Policy, know the following information based on what you plan to configure on the Connections page:

- Asynchronous MDN username and password
- AS2 decryption private key alias and key password
- MDN signature private key alias and key password
- Inbound AS2 sign verify certificate alias

- Inbound MDN sign verify certificate alias
- AS2 endpoint username and password
- AS2 signature private key alias and password
- Outbound AS2 encrypt certificate alias
- Response MDN sign verify certificate alias

AS2 Basic Policy Prerequisites

To use the AS2 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 Generation 2*.
2. Upload the certificate as an X.509 Identity. See Upload an SSL Certificate.
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 AS2 outbound business message.
   - An outgoing asynchronous MDN message sent in response to an inbound AS2 business message.

Create a Connection

Before you can build an integration, you have to create the connections to the applications with which you want to share data.

To create a connection in Oracle Integration:

1. In the left navigation pane, click **Home** > **Integrations** > **Connections**.

2. Click **Create**.

> **Note:**
>
> You can also create a connection in the integration canvas of:
>
> - An orchestrated integration (See Define Inbound Triggers and Outbound Invokes.)
> - A basic routing integration (See Add a Trigger (Source) Connection.)

3. In the Create Connection — Select Adapter dialog, 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 and click

Search.
4. In the Create Connection dialog, 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. Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
   c. 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, let's say 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.
   d. Enter an optional description of the connection.
5. Click **Create**.

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

Configure Connection Properties

Enter AS2 Adapter connection information so your application can process requests.

1. Go to the **Connection Properties** section.
2. In the **AS2 Service URL** field, specify the URL of the trading partner endpoint at which AS2 messages are received.

   This field is only displayed when configuring the AS2 Adapter as an invoke connection. There are no connection properties required when configuring the AS2 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 AS2 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 AS2 Adapter connection by selecting the security policy and associated credentials and certificates.

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 under **Home** > **Settings** > **Certificates**. Upload of only the **X.509 (SSL transport)** type is supported. See Upload an SSL Certificate.

   a. If you select **AS2 Advanced 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 usernames and passwords for AS2 and MDN authentication.

Login Credentials	Comments
• **Username (Async MDN)**: Enter the username used by a trigger connection for authentication when sending an outbound MDN. This is used when asynchronous MDN is requested by an inbound AS2 message. • **Password (Async MDN)**: Enter the password used by a trigger connection for authentication when sending an outbound MDN.	These are optional fields, but are required for sending asynchronous MDN acknowledgments to a partner's secured endpoint.
• **Private Key Alias (AS2 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 under **Home** > **Settings** > **Certificates**. • **Key Password (AS2 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.
• **Private Key Alias (MDN Signature)**: Enter the private key used by a trigger connection to deliver the signed MDN. This is the same key that you upload for the **Identity** category of the **X.509 (SSL transport** type under **Home** > **Settings** > **Certificates**. • **Key Password (MDN Signature)**: Enter the password for the private key used by a trigger connection to deliver the signed MDN.	These are optional fields, but are required for outbound signature generation of MDN acknowledgments.
• **Certificate Alias (Inbound AS2 Sign Verify)**: Enter the partner public certificate used by a trigger connection for inbound AS2 signature verification. This is the same certificate that you upload for the **Trust** category of the **X.509 (SSL transport)** type under **Home** > **Settings** > **Certificates**.	This is an optional field, but is required for inbound signature verification of business messages.
• **Certificate Alias (Inbound MDN Sign Verify)**: Enter the partner public certificate used by a trigger connection for inbound MDN signature verification. This is the same certificate that you upload for the **Trust** category of the **X.509 (SSL transport)** type under **Home** > **Settings** > **Certificates**.	This is an optional field, but is required for inbound signature verification of MDN acknowledgments.
• **Username (AS2 Endpoint)**: Enter the username used by an invoke connection for sending an AS2 message to a protected partner endpoint. • **Password (AS2 Endpoint)**: Enter the password required for sending the AS2 message to the protected partner endpoint.	These are optional fields, but are required for sending business messages to a partner's secured endpoint.

Login Credentials	Comments
• **Private Key Alias (AS2 Signature)**: Enter the private key used by an invoke connection to send a signed AS2 message. This is the same key that you upload for the **Identity** category of the **X.509 (SSL transport)** type under **Home** > **Settings** > **Certificates**. • **Key Password (AS2 Signature)**: Enter the password associated with the private key (AS2 signature) uploaded on the Certificates page under **Home** > **Settings** > **Certificates**.	These are optional fields, but are required for outbound signature generation of business messages.
• **Certificate Alias (Outbound AS2 Encrypt)**: Enter the partner public certificate used by an invoke action for outbound AS2 message encryption. This is the same certificate that you upload for the **Trust** category of the **X.509 (SSL transport)** type under **Home** > **Settings** > **Certificates**.	This is an optional field, but is required for outbound data encryption of business messages.
• **Certificate Alias (Response MDN Sign Verify)**: Enter the partner pubic certificate used by an invoke action for response MDN signature verification. This is the same certificate that you upload for the **Trust** category of the **X.509 (SSL transport)** type under **Home** > **Settings** > **Certificates**.	This is an optional field, but is required for signature verification of synchronous MDN responses in adapter invoke operations.

b. If you select **AS2 Basic 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 under **Home** > **Settings** > **Certificates**. • **Key Password**: Enter the password associated with the private key that you upload on the Certificates page under **Home** > **Settings** > **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.

Login Credentials	Comments
• **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 under **Home** > **Settings** > **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 connection uses a Web Services Description Language (WSDL) file.

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, verify URLs and credentials, and download the diagnostic logs for additional details. Continue to test until the connection is successful.
3. When complete, click **Save**.

Upload an SSL Certificate

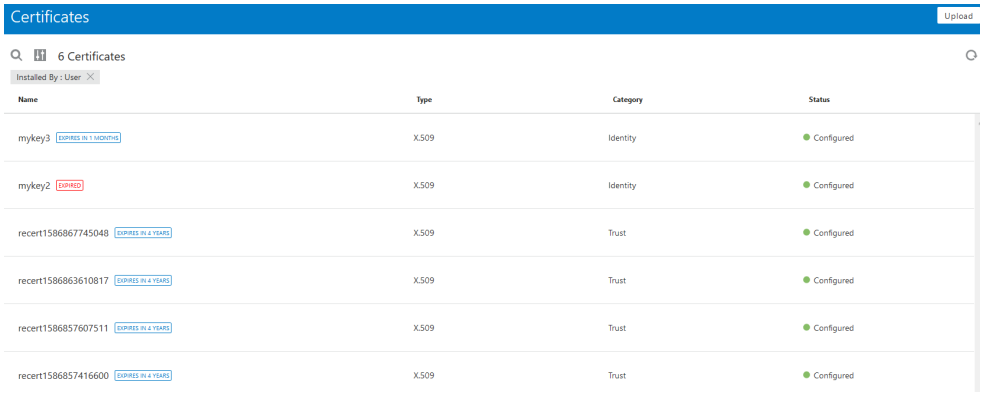
Certificates are used to validate outbound SSL connections. If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception is thrown. In that case, you must upload the appropriate certificate. A certificate enables Oracle Integration to connect with external services. If the external endpoint requires a specific certificate, request the certificate and then upload it into Oracle Integration.

To upload an SSL certificate:

1. In the left navigation pane, click **Home** > **Settings** > **Certificates**.
   All certificates currently uploaded to the trust store are displayed in the Certificates dialog. The

   link enables you 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.



2. Click **Upload** at the top of the page.
   The Upload Certificate dialog box is displayed.
3. Enter an alias name and optional description.
4. In the **Type** field, select the certificate type. Each certificate type enables Oracle Integration to connect with external services.
   - **X.509 (SSL transport)**
   - **SAML (Authentication & Authorization)**
   - **PGP (Encryption & Decryption)**

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.
    c. Click **Upload**.

3

Add the AS2 Adapter Connection to an Integration

When you drag the AS2 Adapter into the trigger or invoke area of an integration, the Adapter Endpoint Configuration Wizard is invoked. This wizard guides you through configuration of the AS2 Adapter endpoint properties.

The following sections describe the wizard pages that guide you through configuration of the AS2 Adapter as a trigger or invoke in an integration.

Topics:

- Basic Info Page
- Trigger Actions Page
- Trigger Identifiers Page
- Invoke Identifiers Page
- Invoke Headers and Packaging Page
- Invoke MDN Options Page
- Summary Page

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.`

Element	Description
B2B Trading Partner mode	**Note**: This option is only available with Oracle Integration Generation 2. Select this option only if you want to: • Create B2B trading partners and agreements in your integration with the AS2 Adapter. See Manage Trading Partners in *Using B2B for Oracle Integration Generation 2*. • Monitor B2B message communication between the trading partners during runtime from the Track B2B Messages page. See Track B2B Messages in *Using B2B for Oracle Integration Generation 2*.
Standalone mode	Select this option to use the AS2 Adapter independent of any trading partners, agreements, or B2B message tracking functionality.

Trigger Actions Page

Select the type of inbound AS2 message for the endpoint to handle.

Element	Description
What type of inbound AS2 messages will this endpoint handle	• **Business Messages**: Select to receive inbound messages such as purchase orders. • **MDN Acknowledgments**: Select to receive the AS2 inbound message delivery notification (MDN) that your partner can send back to acknowledge the messages you sent them.

Trigger Identifiers Page

Specify the Oracle Integration host and remote trading partner AS2 identifiers to validate incoming messages. For incoming messages, all message decompression, signature verification, and decryption actions are handled by the AS2 Adapter trigger connection without the need for you to explicitly configure this security information.

Element	Description
Partner's AS2 Identifier (AS2-From):	Specify the remote trading partner that sends the inbound message.
Host AS2 Identifier (AS2-To):	Specify the Oracle Integration host that receives the inbound message.

Invoke Identifiers Page

Specify the Oracle Integration host and remote partner AS2 identifiers. AS2 identifiers identify trading partners in AS2 transactions.

Element	Description
Host AS2 Identifier (AS2-From):	Specify the Oracle Integration host that sends the message to the remote trading partner.
Partner's AS2 Identifier (AS2-To):	Specify the remote trading partner that receives the message.

Invoke Headers and Packaging Page

Configure the AS2 message for the outbound operation. You can specify message security details such as encryption, signing, and compression.

Element	Description
What is the subject for outbound AS2 messages?	Provide the subject of the message that is sent to the trading partner. You can override this value during runtime by specifying a value in the mapper.
What is the content type of the payload?	Select the payload content type (for example, `application/edi-x12`) to use from the list. To specify a content type that is not available in the list, select **Other Media Type**. This selection activates the **Other Media Type** field for you to enter the value. You can override this value during runtime by specifying a value in the mapper.
Encrypt Outbound Message	Select the checkbox, then select an algorithm from the **Encryption Algorithm** list to use to encrypt the message. The trading partner that receives the message must support the encryption algorithm you select. **Note**: The trading partner's public certificate is required. Ensure that the key is configured on the Connections page.
Sign Outbound Message	Select the checkbox, then select an algorithm from the **Signing Algorithm** list to use to sign the message. The trading partner that receives the message must support the signing algorithm you select. **Note**: A private key is required. Ensure that the key is configured on the Connections page.
Compress Outbound Message	• **Digitally Sign first, then Compress**: Sign the outbound message before compressing it. • **Compress first, then Digitally Sign**: Compress the outbound message before signing it. The order you select is based on what the trading partner that receives the message can support.

Invoke MDN Options Page

Specify if you want the recipient trading partner to send back a message delivery notification (MDN).

Element	Description
What type of MDN will this endpoint request to the trading partner?	• **Sync**: Request that the MDN be sent immediately in the response. • **Async**: Request that the MDN be sent separately from the outbound message. This option requires a separate integration to receive the MDN. • **None**: Request that no MDN be sent back.
Flow Identifier (if **Async** option is selected)	Specify the flow identifier name to receive the asynchronous MDN from the partner. (for example, `AS2_MDN_RECEIVER`). This is the name of a completely separate integration.
Flow Version (if **Async** option is selected)	Specify the complete flow version (for example, `01.00.0000`).
Request the MDN be digitally signed by the trading partner	Select whether the adapter should request a digitally-signed MDN from the trading partner. **Note**: A partner public certificate is required to verify the signed MDN. The certificate to be configured depends on the synchronous or asynchronous MDN type.

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 **Back**. To cancel your configuration details, click **Cancel**.

4

Implement Common Patterns Using the AS2 Adapter

You can use the AS2 Adapter to implement the following common patterns.

Topics:

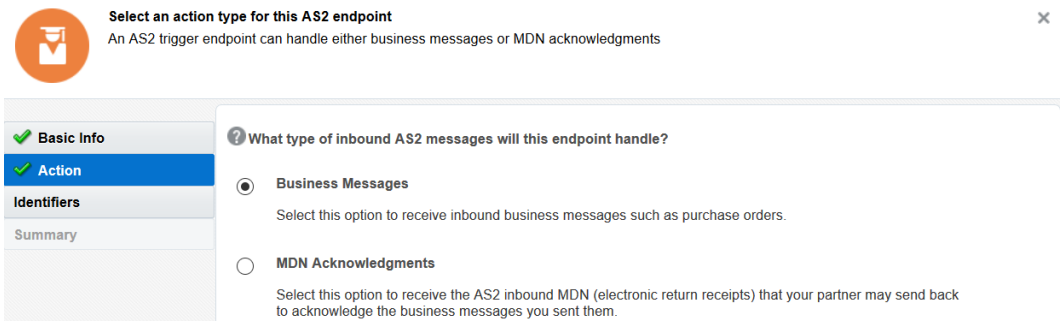
- Receive an EDI Document from a Trading Partner
- Send an EDI Document to a Trading Partner
- Receive an MDN Acknowledgment from a Trading Partner

Receive an EDI Document from a Trading Partner

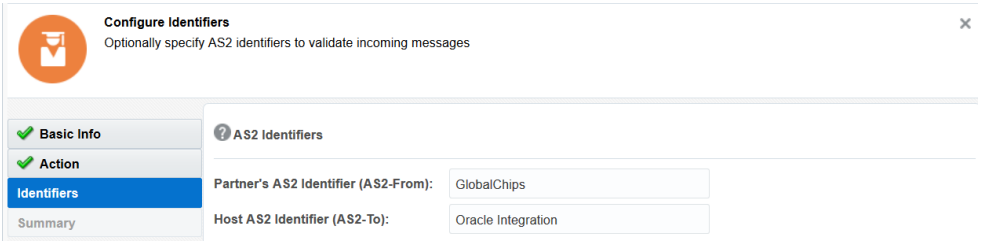
To receive an EDI document in Oracle Integration from a trading partner, you must configure an AS2 Adapter trigger connection to receive business messages. You are asked to optionally specify host and partner AS2 Identifiers for validation.

The trigger connection unpacks the business message and the EDI content is available for further processing with the mapper. EDI content can be read from the element name `content` under `as2_payload` as a base 64-encoded string. To process EDI content as XML, use the EDI translate action for EDI to XML conversion.

1. Drag the AS2 Adapter to the trigger section of the integration canvas.
2. On the Action page, select **Business Messages**.



3. On the Identifiers page, optionally enter the trading partner that triggers the integration in the **Partner's AS2 Identifier (AS2-From)** field and the host trading partner in the **Host AS2 Identifier (AS2-To)** field.



.

See Translate an EDI Document with the EDI Translate Action in *Using Integrations in Oracle Integration Generation 2*.

Send an EDI Document to a Trading Partner

To send an EDI document to a trading partner, you must first get the business document inside the integration boundary using any inbound or outbound adapter. You then configure an AS2 Adapter invoke connection and provide all the necessary details when prompted by the Adapter Endpoint Configuration Wizard. The response is an MDN acknowledgment. It can be immediate or delivered to another integration depending on the type of MDN selection.

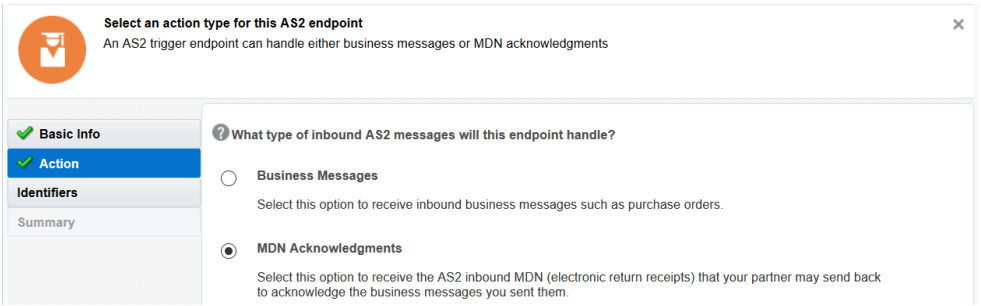
In addition, you map the EDI content to the request mapping of the AS2 Adapter invoke connection. Assuming the EDI content is a base 64-encoded string, if the document is in XML format, translate it with the EDI translate action.

See Translate an EDI Document with the EDI Translate Action in *Using Integrations in Oracle Integration Generation 2*.

Receive an MDN Acknowledgment from a Trading Partner

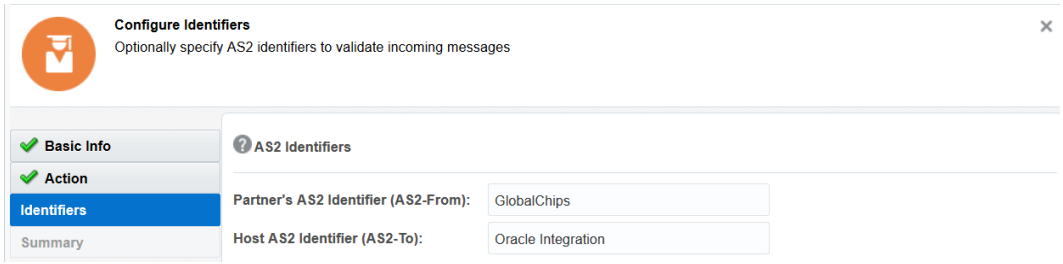
To receive an MDN acknowledgment in Oracle Integration from a trading partner, configure an AS2 Adapter trigger connection to receive MDN acknowledgments. You are prompted to optionally specify the host and partner AS2 identifiers for validation. MDN content is available for further processing with the mapper.

1. Drag the AS2 Adapter to the trigger section of the integration canvas.
2. On the Action page, select **MDN Acknowledgments**.



.

3. On the Identifiers page, optionally enter the trading partner that triggers the integration in the **Partner's AS2 Identifier (AS2-From)** field and the host trading partner in the **Host AS2 Identifier (AS2-To)** field.



.

5

Troubleshoot the AS2 Adapter

Review the following topics to learn about troubleshooting issues with the AS2 Adapter.

Topics:

- Troubleshoot Two-Way SSL Connections

Additional integration troubleshooting information is provided. See Troubleshoot Oracle Integration in *Using Integrations in Oracle Integration Generation 2* and the Oracle Integration Troubleshooting page in the Oracle Help Center.

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 AS2 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.