Oracle® Cloud

Using the Fusion Agent AI Studio Adapter with Oracle Integration 3

G57831-01
September 2026

Oracle Cloud Using the Fusion Agent AI Studio Adapter with Oracle Integration 3,

G57831-01

Primary Author: Oracle Corporation

Contents

About This Content

This guide describes how to configure this adapter as a connection in an integration in Oracle Integration.

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.

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 Fusion Agent AI Studio Adapter

Review the following topics to learn about the Fusion Agent AI Studio 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:

Fusion Agent AI Studio Adapter Capabilities

The Fusion Agent AI Studio Adapter enables you to invoke agents in Oracle AI Agent Studio for Fusion Applications from an integration in Oracle Integration.

Oracle AI Agent Studio for Fusion Applications is Oracle's low-code/no-code platform for creating, extending, testing, deploying, and managing AI agents and multiagent workflows directly within Oracle Fusion Cloud Applications. It allows customers and partners to customize Oracle-delivered agents or build new ones that securely access Oracle Fusion Cloud Applications business data, transactions, APIs, and workflows.

The Fusion Agent AI Studio Adapter provides the following capabilities:

- Enables secure, standards-based communication with agents over the agent-to-agent (A2A) protocol.
- Supports the following operations (actions) to perform against agents.
  - Send message
  - Get task

  For descriptions of these operations, see Basic Info Page.
- Supports accessing the list of available agents in the Fusion Agent AI Studio instance that you specify when configuring your Fusion Agent AI Studio Adapter connection. See Configure Connection Properties.

See AI Agent Studio for Oracle Fusion Cloud Applications and Get Started with AI Agent Studio.

You can configure the Fusion Agent AI Studio Adapter as an invoke connection in an integration in Oracle Integration. The Fusion Agent AI Studio Adapter is one of many predefined adapters included with Oracle Integration. See the Adapters page in the Oracle Help Center.

Fusion Agent AI Studio Adapter Restrictions

Note the following Fusion Agent AI Studio Adapter restrictions.

- Only text-based payloads are currently 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.

Workflow to Create and Add a Fusion Agent AI Studio Adapter Connection to an Integration

You follow a very simple workflow to create a connection with an adapter and include the connection in an integration in Oracle Integration.

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

Step	Description	More Information
1	Decide where to work	• Work in a project (see why working with projects is preferred in *Using Integrations in Oracle Integration 3*). • Work outside a project.
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 a Fusion Agent AI Studio Adapter Connection
3	Create the integration. When you do this, you add trigger (source) and invoke (target) connections to the integration.	Understand Integration Creation and Best Practices in *Using Integrations in Oracle Integration 3* and Add the Fusion Agent AI Studio Adapter Connection to an Integration
4	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in *Using Integrations in Oracle Integration 3*
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 3*
6	Activate the integration.	Activate an Integration in *Using Integrations in Oracle Integration 3*
7	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in *Using Integrations in Oracle Integration 3*

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

2

Create a Fusion Agent AI Studio 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 Fusion Agent AI Studio Adapter.

Prerequisites for Using the JWT User Assertion for OAuth Security Policy

You must satisfy the following prerequisites to create a connection using the JWT User Assertion for OAuth security policy with the Fusion Agent AI Studio Adapter.

Configure a Confidential Application to Use the JWT User Assertion for OAuth Security Policy

You must generate a private key and configure a confidential application to use the JWT User Assertion for OAuth security policy. See Prerequisites for JWT User Assertion in *Using the REST Adapter with Oracle Integration 3*.

Configure the JWT User Assertion for OAuth Security Policy for Outbound Use

- Take the private key you generated in Configure a Confidential Application to Use the JWT User Assertion for OAuth Security Policy and upload it on the Certificates page. See Upload a Certificate to Connect with External Services.
  The service provider typically provides instructions on how to generate the signing keys and the format. For an example, see Required Keys and OCIDs.
- Create the JWT header and JWT payload JSON files. You upload both files on the Connections page when configuring the adapter to support JWT assertions.
  Note the following details about the JWT payload JSON file:
  - The `iss`, `exp`, `sub`, and `aud` claims are mandatory. Oracle Integration validates that these claims are present. Anything else you upload depends on the provider you are trying to call.

- The `iat` (issued at), `exp` (expiry), `nbf` (not before), and `jti` (JWT ID) claims are dynamically calculated if present in the JWT payload JSON file. If you manually provide values for these claims, they are replaced with dynamically-calculated values.
- Any remaining claims are optional and depend upon the provider you are calling.

For example:

JWT Header JSON File Example	JWT Payload JSON File Example

<pre>{
"alg" : "RS256",
"typ": "JWT",
"kid": "fajwt2"
}</pre>
Where:
– `alg`: The algorithm to use.
– `typ`: A JWT assertion typically set to `JWT`.
– `kid`: A key identifier that is uniquely-generated and associated with the uploaded signing key.
	<pre>{
	"iss":
	"f6c9d437eed64e2a8f2b045e39e2e03f",
	"sub": "admin.user",
	"aud": "https://
	identity.oraclecloud.com/",
	"exp": "1739412427"
	"iat": "1727372629"
	"jti": "12345"
	}</pre>
	Where:
	– JWT issuer (`iss`): A unique identifier for the entity that issued the assertion. This is typically the entity that holds the key material used to sign or integrity-protect the assertion. Examples of issuers are OAuth clients (when assertions are self-issued) and third-party security token services. If the assertion is self-issued, the issuer value is the client identifier (`client_id`). If the assertion was issued by a security token service (STS), the issuer must identify the STS in a manner recognized by the authorization server. The assertion must contain an issuer.
	– JWT subject (`sub`): The subject typically identifies an authorized accessor for which the access token is being requested (that is, the resource owner or an authorized delegate). In some cases, this may be a pseudo anonymous identifier or other value denoting an anonymous user. When the client is acting on behalf of itself, the subject must be the value of the client's `client_id`. The assertion must contain a subject.
	– JWT audience (`aud`): A value that identifies the party or parties to process the assertion. The assertion must contain an audience that identifies the authorization server as the intended audience. The authorization server must reject any assertion that does not contain its own identity as the intended audience (in this case, for an Oracle Cloud Infrastructure Identity and Access Management identity domain, `https://identity.oraclecloud.com/`).
	– Expires at (`exp`): The time at which the assertion expires. While the serialization may differ by assertion format, the time must be expressed in UTC format with no time zone component. The assertion must contain an expires-at entity that limits the window during which the assertion can be used. The authorization server must reject expired assertions (subject to allowable

JWT Header JSON File Example	JWT Payload JSON File Example
	clock skew between systems). The authorization server may reject assertions with an expires-at attribute value that is unreasonably far in the future. – Issued at (`iat`): The time at which the JWT was issued. – JWT identifier (`jti`): A unique identifier for the JWT. This helps to prevent replay attacks and ensures the token is only used once.

Prerequisites for Creating a Connection with the Bearer Token Authorization Security Policy

You must satisfy the following prerequisites to create a connection using the Bearer Token Authorization security policy with the Fusion Agent AI Studio Adapter.

Obtain the bearer token value. This value is required when you configure the Fusion Agent AI Studio Adapter on the Connections page.

Create a Connection

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

> **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.
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 **Base URL** field, enter the host name or IP address of the Fusion Agent AI Studio instance from which to invoke agents.

   `https://fusion_agent_ai_studio_instance.com`

3. If you are using the JWT User Assertion for OAuth security policy, expand **Optional properties**, and enter the following:
   - **User**: Enter the user for the JWT subject claim.
   - **Client ID**: Enter the client ID to use in the JWT assertion.

   See Prerequisites for Using the JWT User Assertion for OAuth Security Policy.

Configure Connection Security

Configure security for your Fusion Agent AI Studio Adapter connection.

1. Go to the **Security** section.
2. From the **Security Policy** list, select the policy to use:
   - **JWT User Assertion for OAuth**
   - **Bearer Token Authentication (Deprecated)**
3. If you select **JWT User Assertion for OAuth**, enter the following details:

Element	Description
Access token URL	Enter the URL to which to send a request to obtain the access token. For example: `https://accounts.google.com/oauth2/token`
JWT Private Key Alias	Enter the JWT private key alias. This is the same alias you specified when uploading the signing key certificate on the Certificates page.
Scope	(Optional) Enter the scopes. The scopes define what the application is allowed to access or do on behalf of the user.
Access Token Request	(Optional) Enter the request to obtain the access token. The format you specify can vary by service provider.

   See Prerequisites for Using the JWT User Assertion for OAuth Security Policy.

4. If you select **Bearer Token Authentication (Deprecated)**, enter the following details.

Element	Description
Bearer Token	Enter the generated bearer token.

See Prerequisites for Creating a Connection with the Bearer Token Authorization Security Policy.

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.

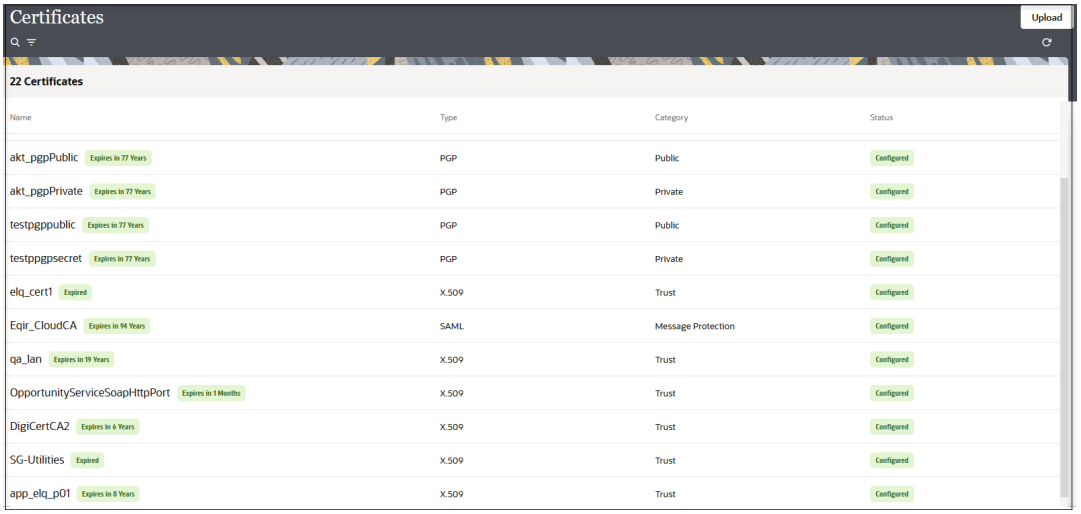
2. Wait for a message about the results of the connection test.
   - If the test was successful, then the connection is configured properly.
   - If the test failed, then edit the configuration details you entered. Check for typos and verify URLs and credentials. Continue to test until the connection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

When you drag the Fusion Agent AI Studio Adapter into the invoke area of an integration, the Adapter Endpoint Configuration Wizard is invoked. This wizard guides you through configuration of the Fusion Agent AI Studio Adapter endpoint properties.

The following sections describe the wizard pages that guide you through configuration of the Fusion Agent AI Studio Adapter as an invoke connection in an integration.

Topics:

Basic Info Page

Specify a name, description, and action to perform.

Element	Description
What do you want to call your endpoint?	Provide a meaningful name so that others can understand the connection. For example, if you are creating a database connection for adding new employee data, you may want to name it `CreateEmployeeInDB`. You can include English alphabetic characters, numbers, underscores, and dashes in the name. You cannot include the following: • Blank spaces (for example, `My DB Connection`) • Special characters (for example, `#;83& or righ(t)now4`) • Multibyte characters
What does this endpoint do?	Enter an optional description of the connection's responsibilities.
Action	Select the operation (action) you want to perform. • **Send message**: Invokes the agent. A message is sent back to the user within the agent conversation. This action is typically used to communicate information, status updates, confirmations, instructions, or results during an agent workflow. This action is part of the agent's interaction layer rather than an external notification mechanism. • **Get task**: Retrieves information about the status of an existing task instance so the agent can inspect or act on it later in the workflow. Typical uses include looking up a task by its task ID or reference, retrieving the task's current status (for example, open, assigned, and completed), and getting task details such as assignee, due date, priority, and task data.

Configuration Page

Select the agent to invoke on the instance.

Element	Description
Provide a key word to search the agent and press enter	Enter a keyword after the **%** to filter the display of agents. For example, enter `OIC1` to show agents that begin with those letters.
Select Agent	Displays the list of the agents available in the instance that you specified when configuring the Fusion Agent AI Studio Adapter connection. Select the agent appropriate to your business requirement. See Configure Connection Properties.

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 Fusion Agent AI Studio Adapter

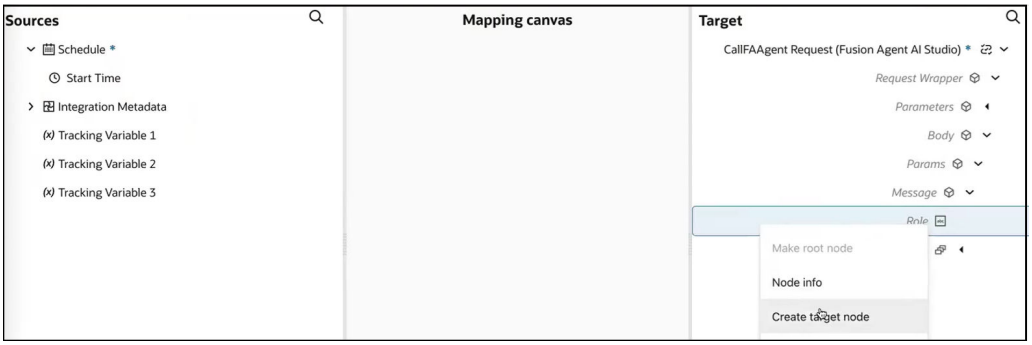
You can use the Fusion Agent AI Studio Adapter to implement the following common pattern.

Topics:

Invoke an Agent and Get Agent Status in Oracle AI Agent Studio for Fusion Applications

Use the Fusion Agent AI Studio Adapter to invoke an agent in Oracle AI Agent Studio for Fusion Applications and return the agent status. This use case provides a high level overview of the steps required to achieve this goal.

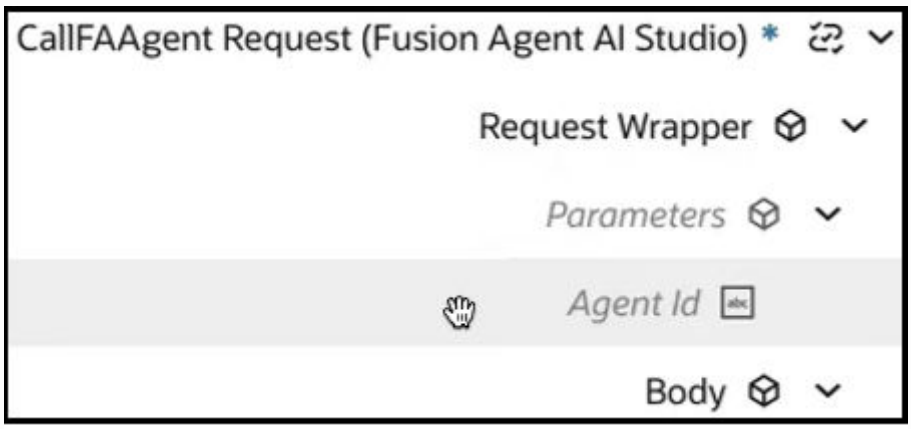
1. Configure a Fusion Agent AI Studio Adapter connection. See Create a Fusion Agent AI Studio Adapter Connection.
2. Create a schedule integration.
3. Drag the Fusion Agent AI Studio Adapter into the integration canvas.
4. Configure the Fusion Agent AI Studio Adapter as follows:
   a. On the Basic Info page, provide a name (for this example, **CallFAAgent** is specified) and select **Send message** from the **Actions** list. This selection invokes an agent.
   b. On the Configuration page, select the **OIC1PAYABLESTEAM1** agent from the **Select Agent** list. This is the agent to invoke.
   c. On the Summary page, review your selections.
5. In the mapper, map the prompt and payload to invoke the selected agent:
   a. Expand the target section.
   b. Right-click **Role**, and select **Create target node**.



   c. In the Expression Builder, specify `"user"` for the **Role** element.

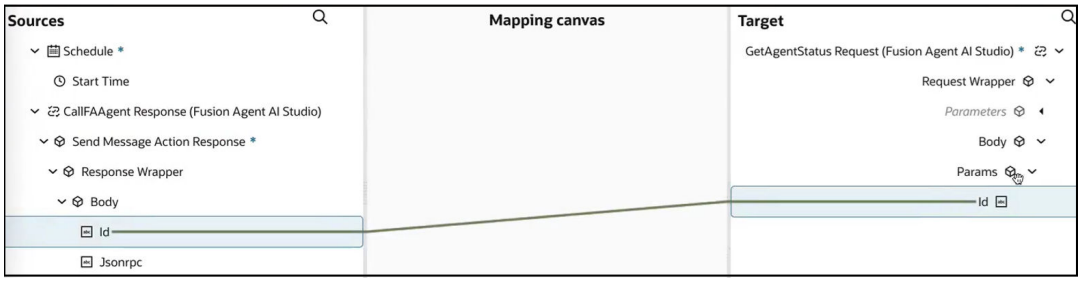
d. Right-click **Text**, and select **Create target node** to specify the content for your prompt.

e. In the Expression Builder, specify the prompt `"Check the files in my invoices folder"` for the **Text** element.

> **Note**
>
> While not demonstrated in this use case, the **Agent Id** target parameter can be used to override the agent you selected on the Configuration page in the Adapter Endpoint Configuration Wizard.
>
> 
>

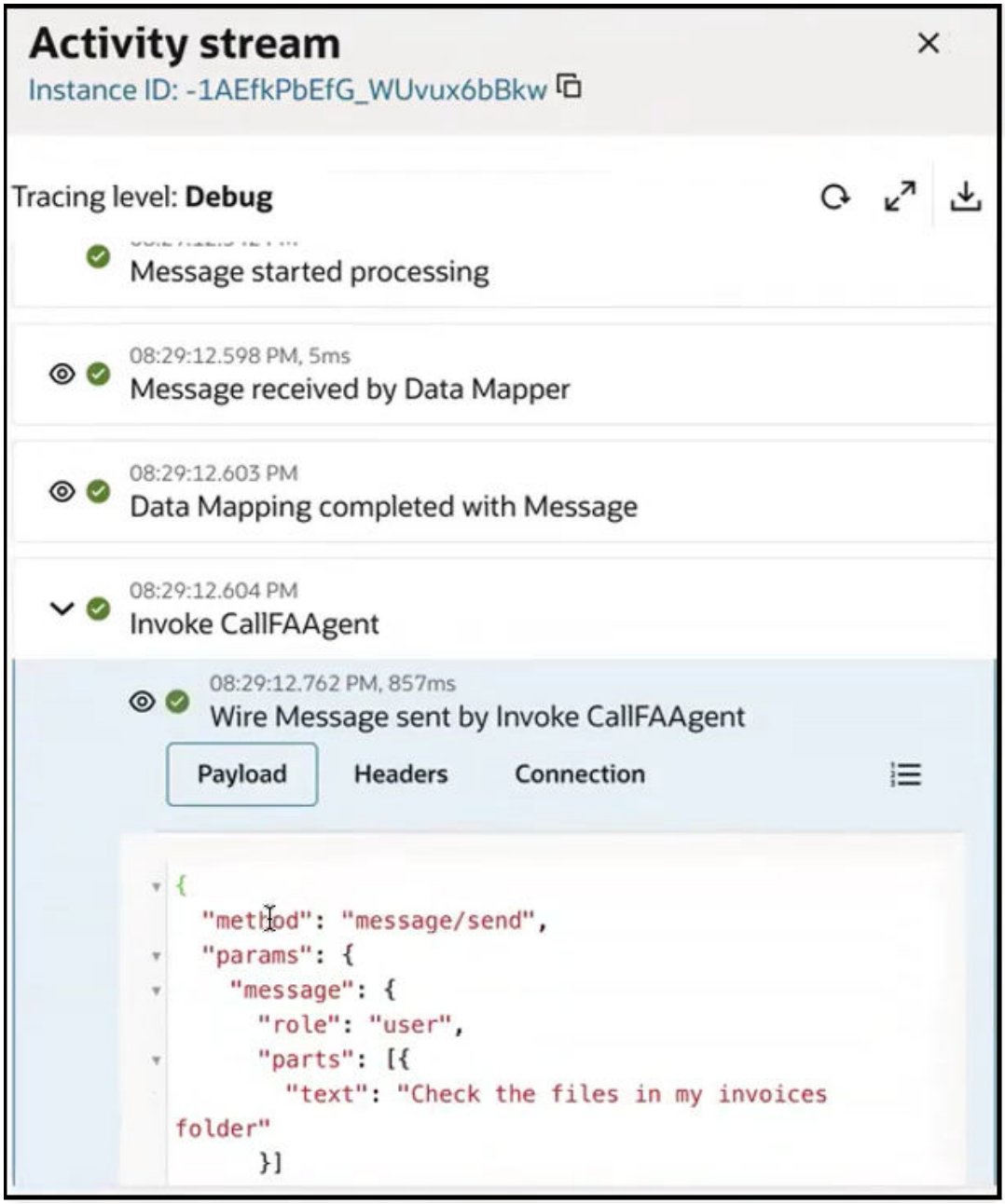
6. Add and configure a wait action to wait 60 seconds for the agent to complete the initial operation before beginning the second operation to return the agent status.

7. Drag a second Fusion Agent AI Studio Adapter below the wait action in the integration canvas.
8. Configure the Fusion Agent AI Studio Adapter as follows:
   a. On the Basic Info page, provide a name (for this example, **gettaskstatusofagent** is specified) and select **Get task** from the **Actions** list. This selection gets the status of the agent.
   b. On the Configuration page, again select the **OIC1PAYABLESTEAM1** agent from the **Select Agent** list.
   c. On the Summary page, review your selections.
9. In the second mapper, map the ID of the agent that was invoked in the first Fusion Agent AI Studio Adapter connection:

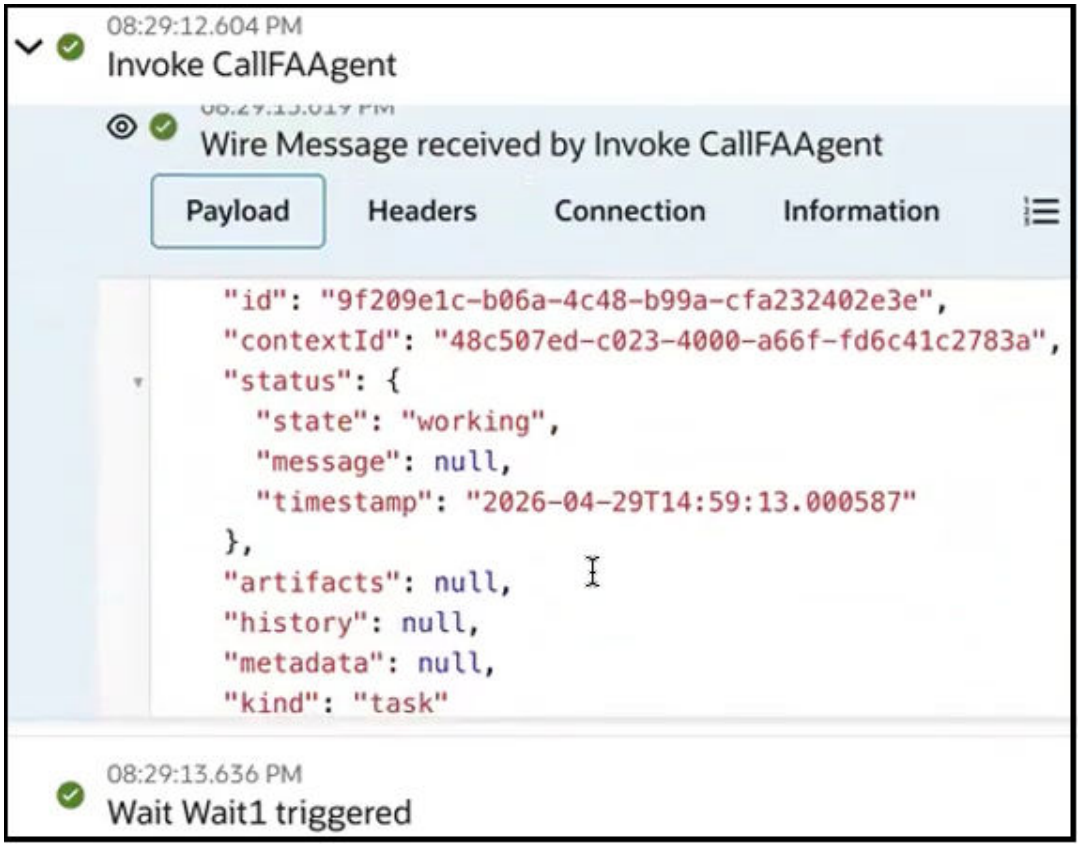


10. Specify the tracking variable.
    a. Click **Business Identifiers** (I).
    b. Drag the required variable to use for the tracking reference (for this example, **startTime** is selected because this is a schedule integration).
11. Activate the integration.
12. From the **Actions** ⋮ menu of the integration, select **Run**.
13. Select **Ad hoc request**, and click **Run**.
14. Expand the activity stream to view the first Fusion Agent AI Studio Adapter connection.

    The request message sent by the Fusion Agent AI Studio Adapter connection shows the role and prompt text you specified in the mapper.



The response received by the Fusion Agent AI Studio Adapter connection shows the state as `working`.



15. Wait 60 seconds for the wait action to complete.
16. Expand the activity stream to view the second Fusion Agent AI Studio Adapter connection.

    The state is now `completed`.

17. Scroll down further in the activity stream for that connection and note the text received from the agent in response to the initial prompt. The agent has responded with a followup question asking for more details.