

Oracle Fusion Cloud Transportation and Global Trade Management

AI Guide

26B



Oracle Fusion Cloud Transportation and Global Trade Management
AI Guide

26B

G56728-01

Copyright © 2026, Oracle and/or its affiliates.

Author: Oracle Transportation and Global Trade Management Product Team

Contents

Get Help	i
<hr/>	
2 Introduction	3
Audience	3
Prerequisites	3
3 Generating Public/Private Keys with a Certificate	5
Generating Public/Private Keys with a Certificate	5
4 Working in OTM IDCS	7
Creating a Confidential Application in OTM IDCS	7
Importing a Certificate into IDCS of OTM	15
5 Working in AI Agent Studio	17
Creating OTM Users in AI Agent Studio	17
6 Working in Fusion IDCS	19
Creating Confidential Application in Fusion IDCS	19
Importing Public Key on IDCS of Fusion POD	24
7 Working in AI Agent Studio Data Sources	27
Creating the AI Agent Studio Data Source	27
8 Working in OTM	31
Setting up AI Agentic Trusts	31
Adding Access Control Lists to Users	32

Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

Get Help in the Applications

Use help icons to access help in the application.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, and watch events.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to otm-doc_us@oracle.com.

Thanks for helping us improve our user assistance!

2 Introduction

Audience

The purpose of this document is to help you get started with using Oracle's AI Agent Studio and Transportation and Global Trade Management Cloud Services. It provides details on how to integrate Oracle AI (Artificial Intelligence) Agent Studio with Oracle Transportation and Global Trade Management (OTM) REST APIs using secure and compliant OAuth 2.0 patterns.

- IDCS Admins for OTM and AI Agent Studio
- OTM Admins

It's important to follow the chapters in the guide in order. If you don't follow this order, you might see connections issues between OTM and AI Agent Studio.

Prerequisites

Before completing this guide, you **must** have the following:

- Access to create keys and certificates using OpenSSL or another tool.
- ADMIN access to Fusion's Identity Cloud Service (IDCS).
- ADMIN access to OTM's Identity Cloud Service (IDCS).
- ADMIN access to AI Agent Studio.
- Any 26B Fusion module which comes with AI Agent Studio.
- An OTM 26B instance.
- DBA.ADMIN or equivalent access to the OTM instance.

While completing the setup detailed in this guide, you will need to take note of certain information as it will be needed later in the setup. Use the following tables to make a note of the required information. In this guide, you will see a note following the required information asking you take note of the value to be reused in a later step.

Tip: Print this page so you can use it to record your work as you progress through this guide. Write down all the values you create when instructed to by the guide so you can easily reference them later.

Key and Certificate to Remember

Field Name	Value
certificate For example, <code>jwt-signing.crt</code>	

Field Name	Value
public key For example, <code>jwt-signing.key</code>	

Remember from IDCS of OTM

IDCS of OTM Field Name	Value
IDCS of OTM confidential app Name	
IDCS of OTM confidential app Primary audience	
IDCS of OTM confidential app certificate Alias	
IDCS of OTM confidential app Scope	

Remember from IDCS of Fusion

IDCS of Fusion Field Name	Value
IDCS of Fusion confidential app Name	
IDCS of Fusion confidential app certificate Alias	
IDCS of Fusion confidential app Scope	
IDCS of Fusion confidential app Client ID	

3 Generating Public/Private Keys with a Certificate

Generating Public/Private Keys with a Certificate

Digital certificates and cryptographic keys are used to establish secure, authenticated communication between AI Agent Studio and OTM applications via OAuth 2.0 JSON Web Token (JWT) assertions. You need a private key, public key, and certificate.

You can use the OpenSSL command utility to generate the keys and the certificate as shown in the example below; however, you can use the tool that is supported within your organization.

1. In OpenSSL, generate the private key with a certificate by running the following command:

```
openssl req -newkey rsa:4096 -subj "/CN=spectra-service" -x509 -sha256 -days 365 -nodes -out "./jwt-signing.crt" -keyout "./jwt-signing.key"
```

Note: In the *Prerequisites*, write down the **certificate**. You will need it later.

2. In OpenSSL, generate the public key by running the following command:

```
openssl pkey -in jwt-signing.key -pubout -out jwt-signing.pub
```

Note: In the *Prerequisites*, write down the **public key**. You will need it later.

The same key, `jwt-signing.key`, and certificate, `jwt-signing.crt`, can be used in multiple locations during this guide as listed below:

- Identity Cloud Service (IDCS) of OTM confidential app
- IDCS of Fusion confidential app
- AI Agent Studio data source
- OTM Agentic Trust page

However, you should follow your company's standards.

The key is used by both confidential apps to sign JWT assertions and used in the private key field of the AI Agent Studio data source application.

The certificate is uploaded to Fusion's Identity Cloud Service (IDCS) and used in the public key field of the AI Agent Studio data source application.

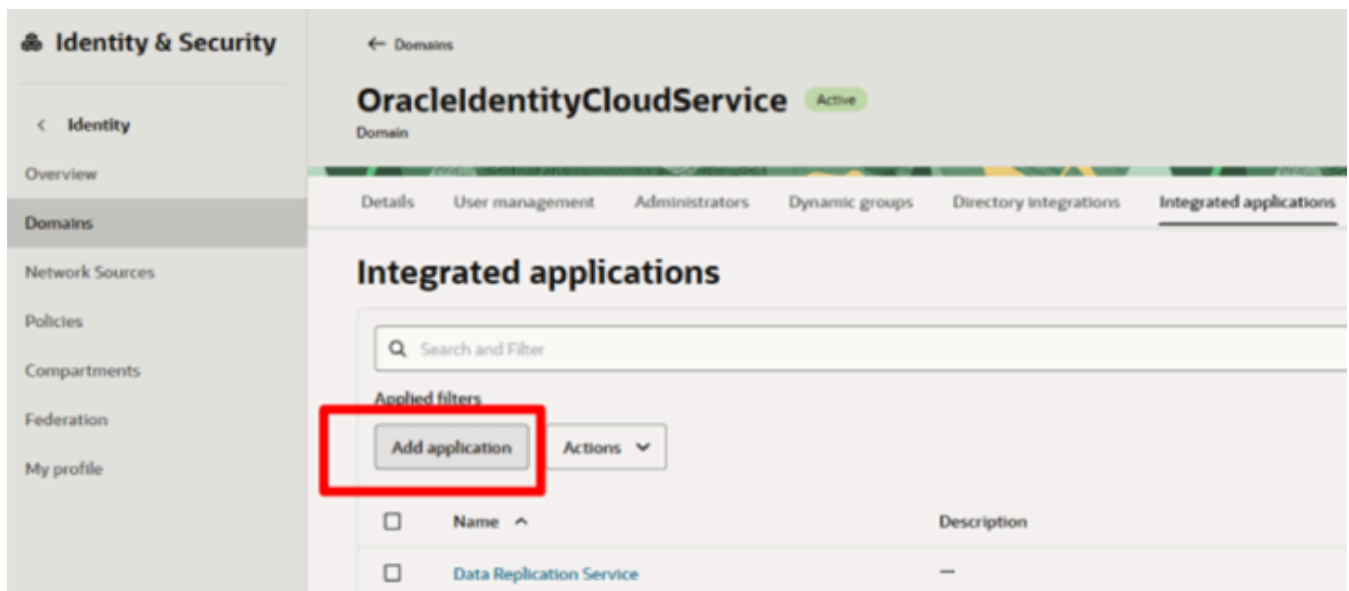
4 Working in OTM IDCS

Creating a Confidential Application in OTM IDCS

The OTM-side confidential application registers OTM as a trusted resource server and validates tokens presented by AI Agent Studio, thus enforcing secure authentication and access.

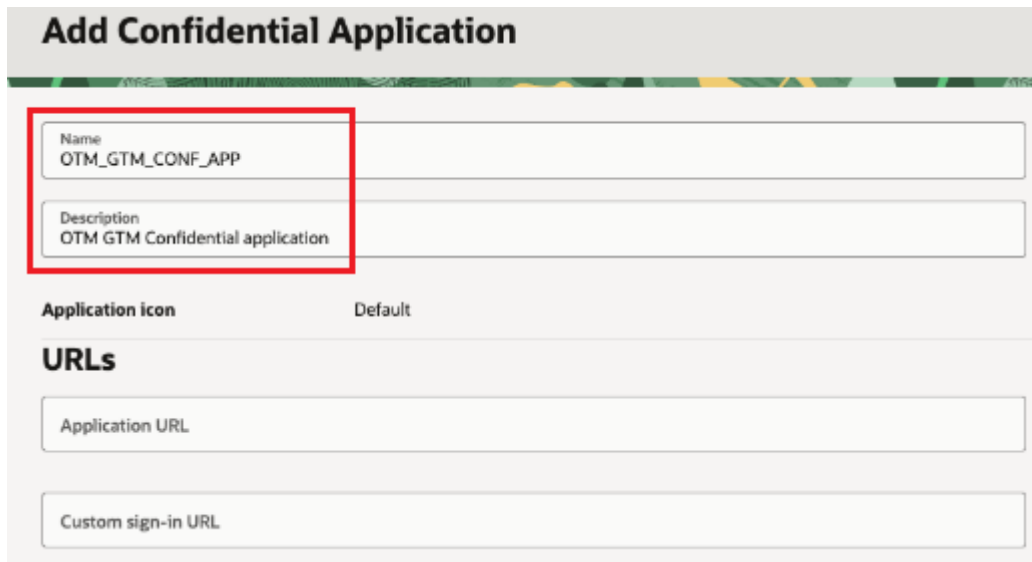
An example of creating the OTM-side confidential application using OTM's IDCS is shown below.

1. Sign in to the **OTM IDCS Admin Console**.
2. On the **Welcome** page, select **Take me there** to go to the Identity Domain.
3. Navigate to **Identity > Domains**.
4. On the Domain page, select **Integrated applications**. This page is where you'll add an OAuth2 confidential client application.
5. Select **Add application**.



6. On the next page, select **Confidential Application** and select **Launch workflow**.

7. On the Add Confidential Application page, provide a unique application **Name** (for example `OTM_GTM_CONF_APP`) and a **Description**.



Add Confidential Application

Name
OTM_GTM_CONF_APP

Description
OTM GTM Confidential application

Application icon Default

URLs

Application URL

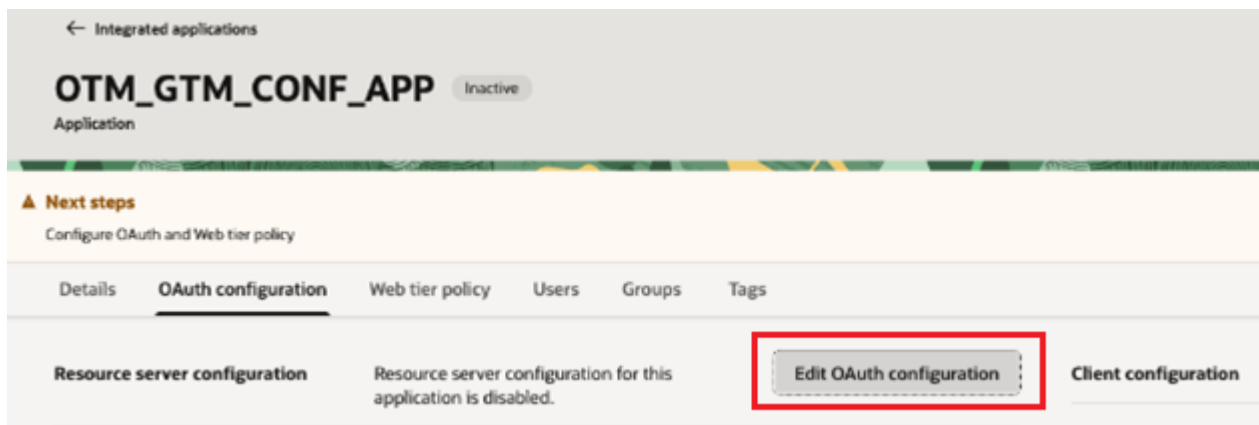
Custom sign-in URL

Note: In the *Prerequisites*, write down the **OTM IDCS confidential app Name**. You will need it later.

8. Select **Submit**. A new confidential application is created.

On the new application screen now configure OAuth as follows:

9. Select the **OAuth configuration** tab.
10. Select **Edit OAuth configuration**.



← Integrated applications

OTM_GTM_CONF_APP Inactive
Application

Next steps
Configure OAuth and Web tier policy

Details **OAuth configuration** Web tier policy Users Groups Tags

Resource server configuration Resource server configuration for this application is disabled. **Edit OAuth configuration** Client configuration

The OTM confidential application needs to be configured both as a Resource Server and Client Configuration. First, add a resource server.

11. In the **Resource server Configuration** section, select the **Configure this application as a resource server now** option. The page will change to show more fields.

12. Enter a **Primary audience** to protect the OTM APIs. The primary audience should be your OTM instance URL (For example, `https://<otm_host_name>`).

The screenshot shows the 'Edit OAuth configuration' interface. Under the 'Resource server configuration' section, the 'Configure this application as a resource server now' option is selected. Below this, there is a section for 'Configure application APIs that need to be OAuth protected'. This section includes a dropdown for 'Access token expiration (seconds)' set to 3600, a toggle for 'Allow token refresh' which is currently off, and a text input field for 'Primary audience'. The 'Primary audience' field is highlighted with a red box. Below the 'Primary audience' field, there are sections for 'Add secondary audience' and 'Add scopes', both with their respective toggle switches turned off.

Note: In the *Prerequisites*, write down the **IDCS of OTM confidential app Primary audience** which is the URL of your OTM instance. You will need this later.

Next, you add a scope.

13. Scroll down and select the **Add scopes** option.

14. Select **Add** in the **Scopes** section.

Edit OAuth configuration

Add secondary audience

Enter the secondary recipients where the access token of your application is processed.

Add scopes

Add scopes to specify which of the application's resources are available to other applications.

Scopes

Search and Filter

Add Remove

Scope	Protected	Display name	Description
No items to display			

Create new items or search again using different filters or search terms.

15. Add a **Scope** (for example, `OTM_GTM_CONF_APP`) and a **Description**.

Add scope

Scope
OTM_GTM_CONF_APP

Display name

Description
OTM GTM Scope

Requires user consent

Require consent for this scope configured for the application.

Note: In the *Prerequisites*, write down the **IDCS of OTM confidential app Scope**. You will need this later.

16. Select **Add**.

Next, enable Client Configuration for this OAuth application.

17. With the new scope added, select the **Submit** button.

You need to submit the OAuth configuration and then edit it again to see the scope that you just added.

18. Select the **Edit OAuth configuration** button.

19. Scroll down to the **Client Configuration** section and check the **Configure this application as a client now** option.

20. Select the allowed grant types of **Resource owner**, **Client credentials**, and **JWT assertion**.

Edit OAuth configuration

> **Resource server configuration**

✓ **Client configuration**

Configure this application as a client now

No client configuration

Authorization

Allowed grant types
Select the grant types that this application is allowed to use when requesting validation.

Resource owner

Client credentials

JWT assertion

Refresh token

Device code

Authorization code

Implicit

SAML2 assertion

TLS client authentication

21. Scroll down and select **Import certificate**.

Client type
Select the client type. Choose Trusted if the client can generate self-signed user assertions, and then import your signing certificate.

Trusted

Confidential

Certificate

Alias

Import certificate

Allowed operations
Select 'Introspect' if you want to allow access to a token introspection end point for your application. Select 'On behalf of' if you want to ensure that access privileges can be generated from the user's privileges alone. Using this option means that a client application can access endpoints to which the user has access, even if the client application by itself wouldn't normally have access.

Introspect

On behalf of

ID token encryption algorithm
None

Bypass consent

Cancel Submit

22. Add an **Alias** for the certificate. For example, `otm_gtm` .

Note: In the *Prerequisites*, write down the **IDCS of OTM confidential certificate Alias**. You will need this later.

23. Use the **Drop a file or select one** field to upload the certificate. Upload the certificate `jwt-signing.crt` that was created earlier.

Note: Import the certificate that you created earlier. *Generating Public/Private Keys with a Certificate*

24. Once the certificate is uploaded, select **Import**.

Import certificate

Alias
OTM_GTM

Certificate file

Drop a file or select one
File formats supported: .pem, .cer, .crt, .der

File upload Clear

jwt-signing.crt 1.1 KIB ×

25. Scroll down and select **Add resources**.
26. Select **Add scope**.

Add resources

Add resources if you want your application to access the APIs of other applications.

Resources

Search and Filter

Add scope Remove

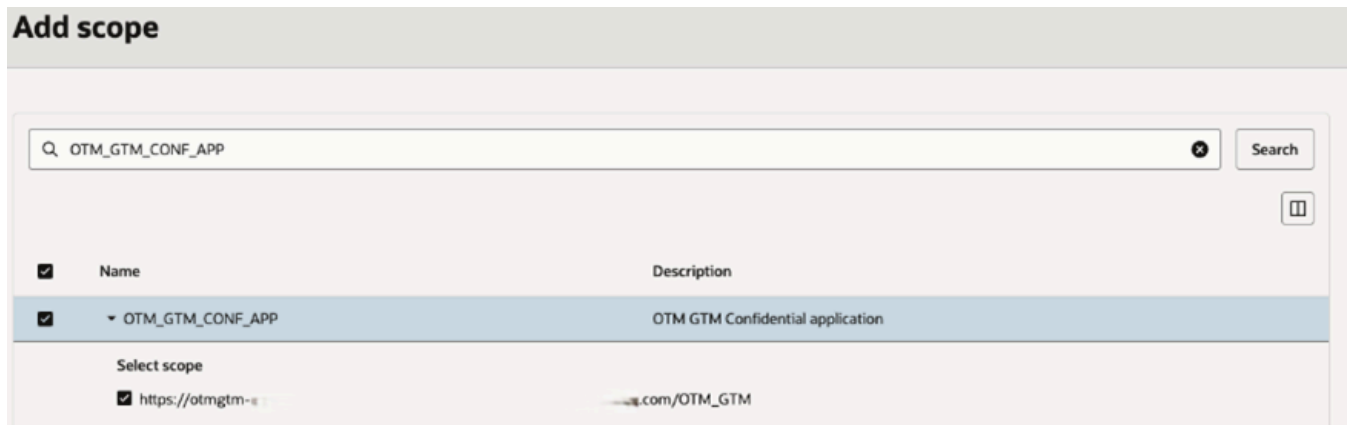
Resource	Protected
No items to display	

Create new items or search again using different filters or search terms.

27. Under **Add scope**, select the **Scope** created previously.

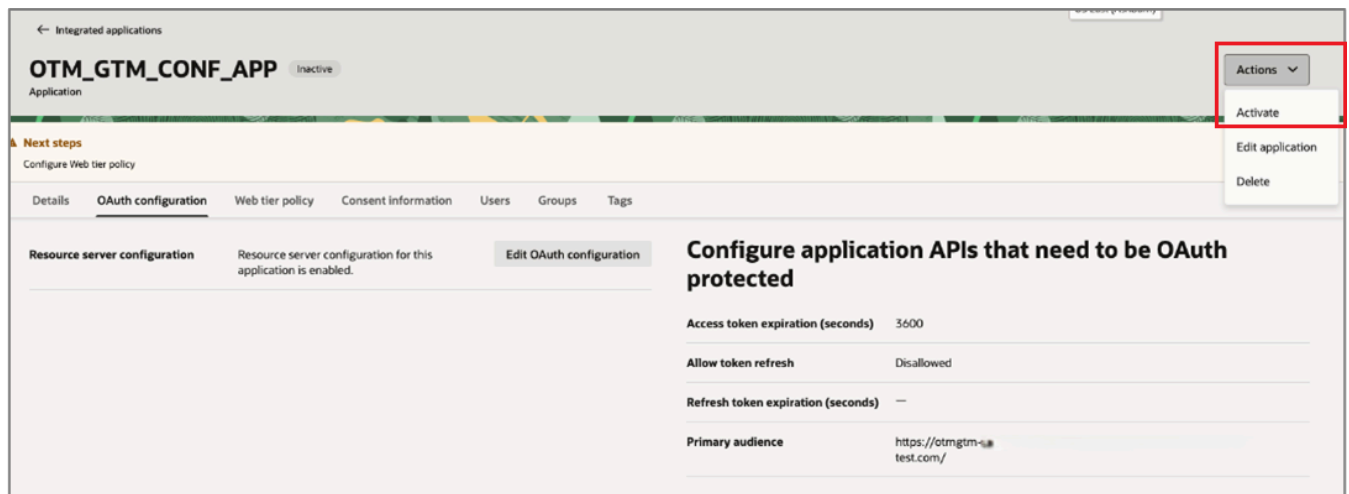
Note: Use the value that you wrote down for the **IDCS of OTM confidential app Scope** in *Prerequisites*.

28. Select **Add**.



29. Select the **Submit** button to complete the OAuth set up.

30. Select **Actions** and select **Activate**.



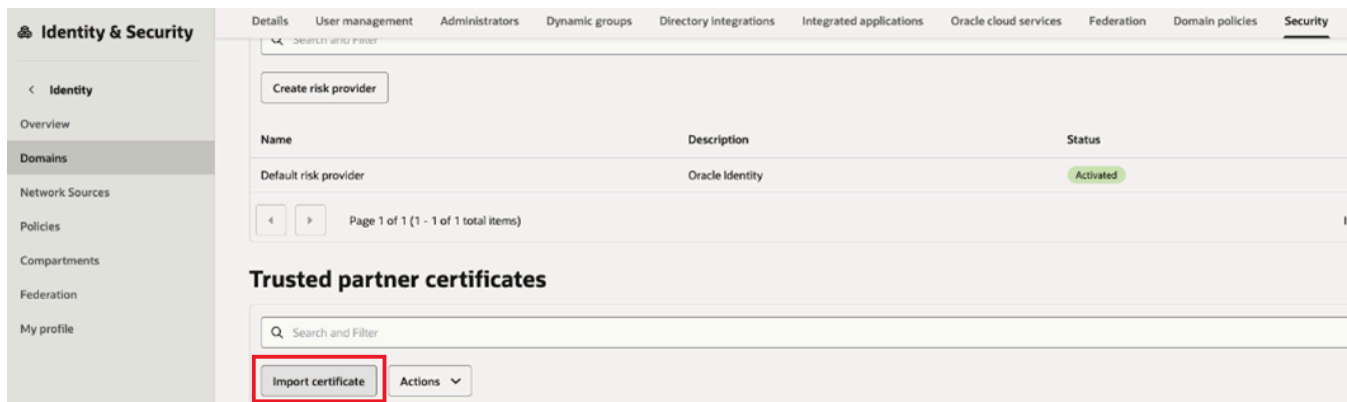
31. On the Activate application message, select **Activate application**.

Note: The OTM confidential app is configured to trust tokens signed by the correct certificates issued from the AI Agent.

Note: The setup ensures that only authorized calls from AI Agent Studio can reach OTM REST endpoints.

Importing a Certificate into IDCS of OTM

1. Sign in to the **Admin Console in the IDCS of OTM**.
2. Go to the **Security** tab of the default domain.
3. Select **Import certificate**.



4. For the name enter the same **Alias** created previously.

Note: Use the value that you wrote down for the **IDCS of OTM confidential app certificate Alias** in *Prerequisites*.

5. Select **Drop a file or select one**.
6. Select the **file used in the previous section**.

Note: Import the certificate that you created earlier. *Generating Public/Private Keys with a Certificate*

7. Select **Import**.

Import certificate

[Learn more.](#)

Alias
OTM_GTM

Certificate

Drop a file or select one
File formats supported: .pem, .cer, .crt, .der

File upload Clear

jwt-signing.crt	1.1 KIB	×
-----------------	---------	---

5 Working in AI Agent Studio

Creating OTM Users in AI Agent Studio

You need to create users in the AI Agent Studio confidential app that corresponds to your users in OTM.

Note: The OTM user Nickname must be the same as the user name in AI Agent Studio.

To create users in AI Agent Studio, follow these steps:

1. Sign in to **AI Agent Studio** with Admin Privileges.
2. Select the **home** button.
3. Navigate to **Tools > Security Console**.
4. Select **Users**.
5. Search for **SCMOPERATIONS**, **SCMIMPL** or an **admin user** that provides you with the appropriate roles for use with AI Agent Studio and OTM.
6. For that user, select **action** button and **copy** the user.
7. Enter the following information for the user:
 - o first name
 - o last name
 - o user name
 - o email ID
 - o password (twice)
8. Save the new user.

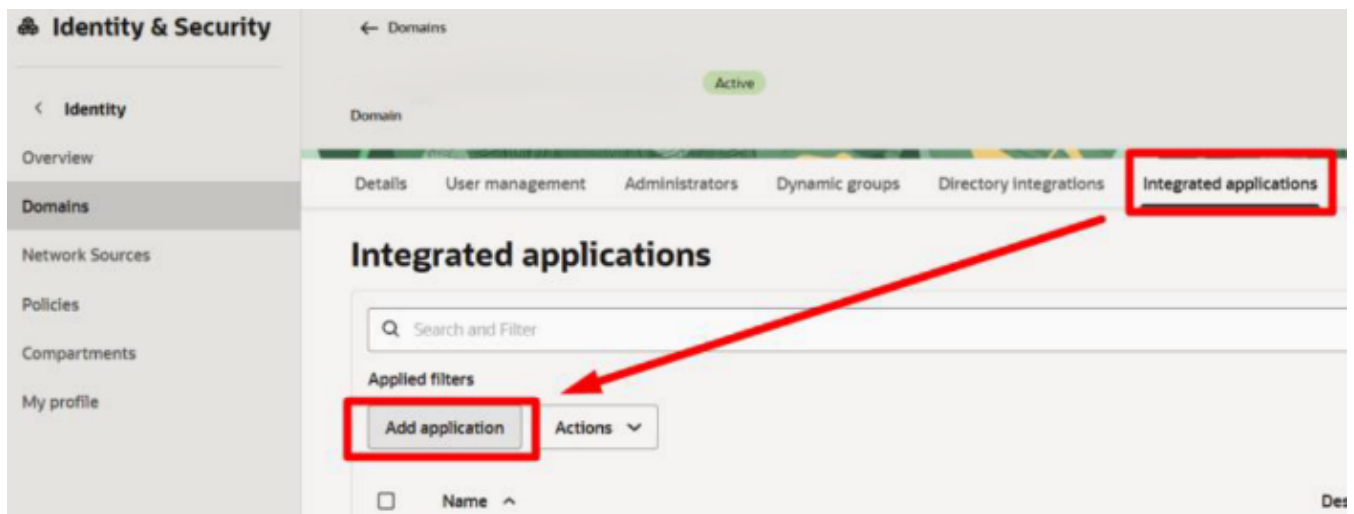
6 Working in Fusion IDCS

Creating Confidential Application in Fusion IDCS

A confidential application in Identity Cloud Service (IDCS) represents the AI Agent Studio and acts as the OAuth 2.0 client. This allows the agent to programmatically obtain access tokens required to call OTM REST APIs securely.

An example of creating the confidential application in Fusion's IDCS is shown below.

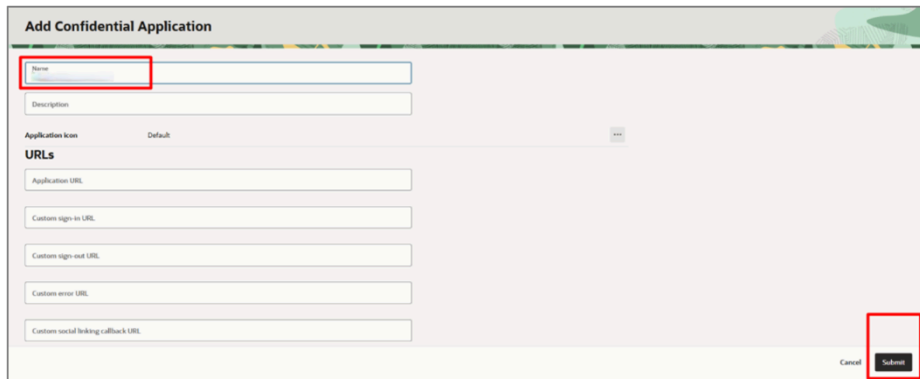
1. Sign in to the **Fusion IDCS Console** as a valid **admin user**.
2. On the **Welcome** page, select **Take me there** to go to the Identity Domain.
3. Navigate to **Identity > Domains**.
4. On the Domain page, select **Integrated applications**. This page is where you'll add an OAuth2 confidential client application.
5. Select **Add application**.



6. On the next page, select **Confidential Application** and select **Launch workflow**.

7. On the Add Confidential Application page, provide a unique application **Name** and a **Description**.

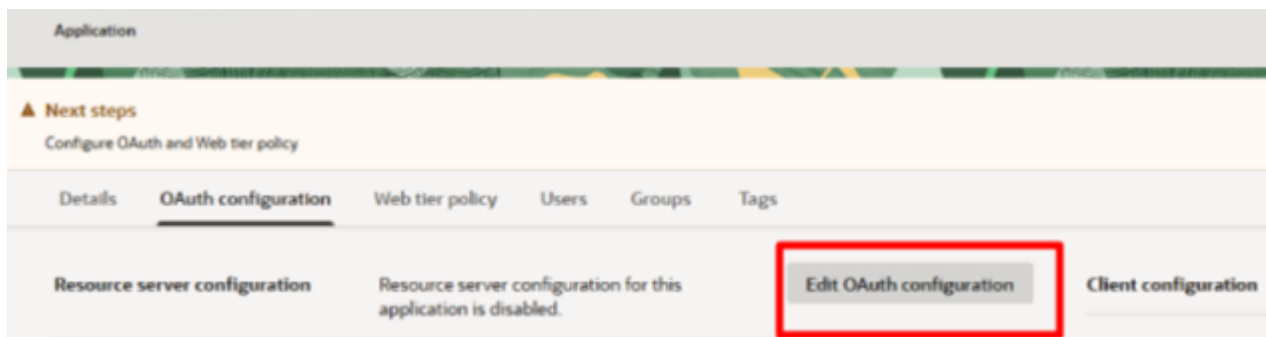
Note: In the *Prerequisites*, write down the **IDCS of Fusion confidential app Name**. You will need it later.



8. Select **Submit**.

A new confidential application is created. On the new application page, you'll configure OAuth.

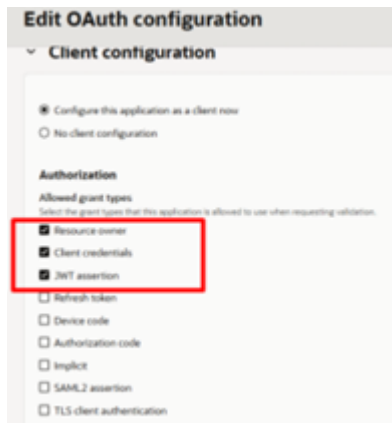
9. Select the **OAuth configuration** tab.
10. Select **Edit OAuth configuration**.



Next, enable Client Configuration for this OAuth application.

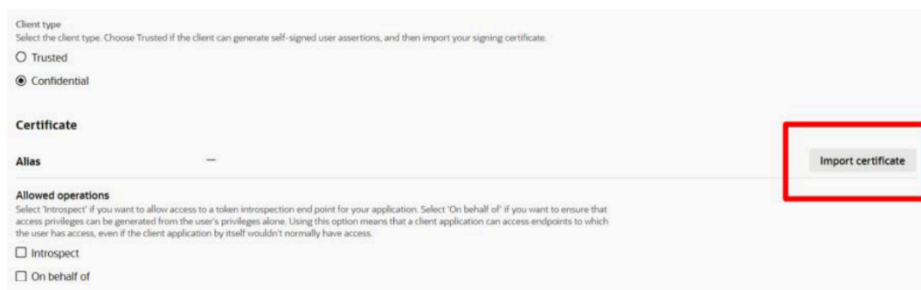
11. Scroll down to the **Client Configuration** section and select the **Configure this application as a client now** option.

12. Select the allowed grant types: **Resource owner**, **Client credentials**, and **JWT assertion**.



Scroll down and import the certificate generated previously.

13. Select **Import certificate**.



14. Add a certificate **Alias**. For example, OTM_GTM.

Note: In the *Prerequisites*, write down the **IDCS of Fusion certificate Alias**. You will need it later.

15. Use the **Drop a file or select one** field to upload the certificate. Upload the file `jwt-signing.crt` that was created earlier.

Note: Import the certificate that you created earlier. *Generating Public/Private Keys with a Certificate*

16. Once the certificate is uploaded, select **Import**.

Import certificate

[Learn more.](#)

Alias

Certificate

Drop a file or select one
File formats supported: .pem, .cer, .crt, .der

File upload Clear

jwt-signing.crt 1.1 KIB ×

17. Select the **On behalf of** checkbox.
18. Select the **Bypass consent** checkbox.

Edit OAuth configuration

Confidential

Certificate

Alias

Allowed operations
Select 'Introspect' if you want to allow access to a token introspection end point for your application. Select 'On behalf of' if you want to ensure that access privileges can be generated from the user's privileges alone. Using this option means that a client application can access endpoints to which the user has access, even if the client application by itself wouldn't normally have access.

Introspect

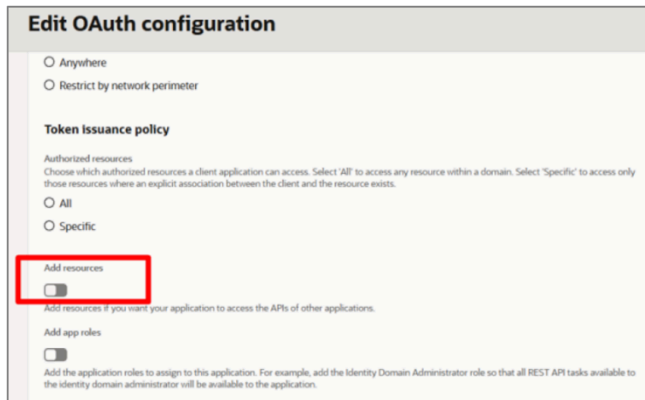
On behalf of

ID token encryption algorithm
None

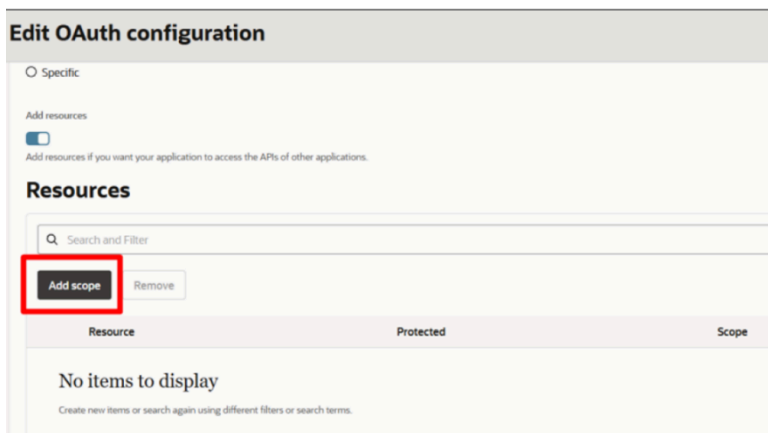
Bypass consent

Turn on bypass consent to overwrite the Require consent attribute for all the scopes configured for the application. Turning this option on means that no scope will require consent.

19. Scroll down and turn on **Add resources**.

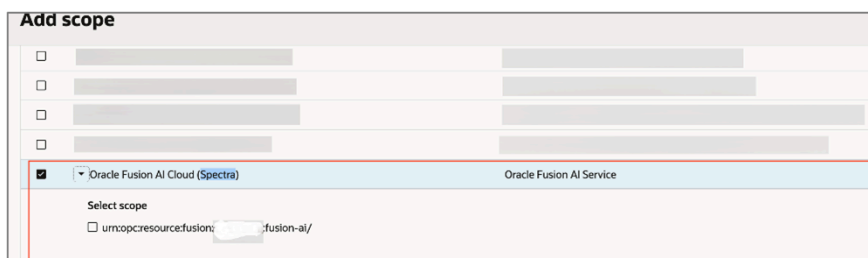


20. Scroll down and select the **Add scope** button.



Next, add the AI Agent Studio scope to the confidential application.

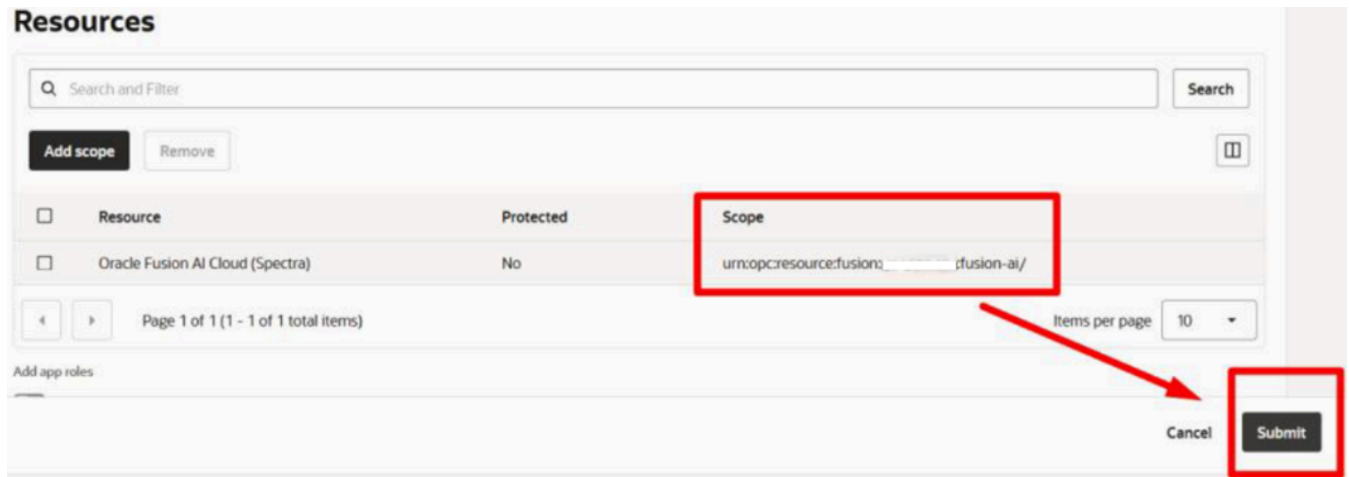
21. Under **Add scope**, select the AI Agent Studio scope with a Name of **Oracle Fusion AI Cloud (Spectra)**.



Note: The **Oracle Fusion AI Cloud (Spectra)** scope is created automatically if you have a Fusion instance. If you do not see this scope, then contact your Fusion contact or Fusion Support.

Note: Use the value that you wrote down for the **IDCS of Fusion confidential app Scope** in *Prerequisites*.

22. Confirm the **Scope** similar to `urn:opc:resource:fusion:<fusionservername>:fusionai/`.



23. Select the **Submit** button.

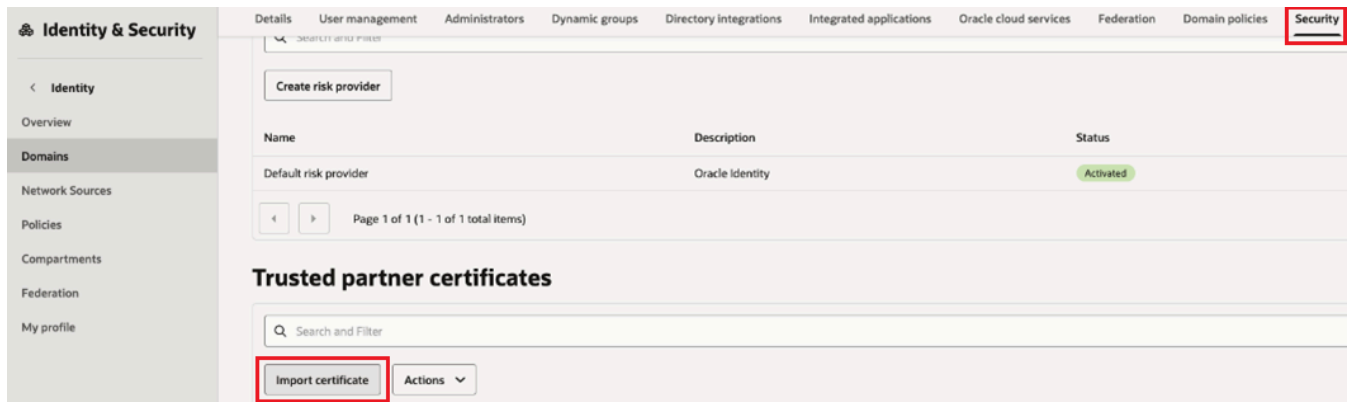
Note: In the *Prerequisites*, write down the **IDCS of OTM confidential app Client ID**. You will need it later.

24. Select **Actions** menu and select **Activate**.
25. On the Activate application message, select **Activate application**.

Importing Public Key on IDCS of Fusion POD

1. Sign in the **Admin Console of IDCS of Fusion**.
2. Go to the **Security** tab of the default domain.

3. Select **Import Certificate**.



4. For the name enter the **same alias used in the previous section**.

Note: Use the value that you wrote down for the **IDCS of OTM confidential app certificate Alias** in *Prerequisites*.

5. Select **Drop a file or select one**.

6. Select the **file used in the previous section**.

7. Select **Import**.

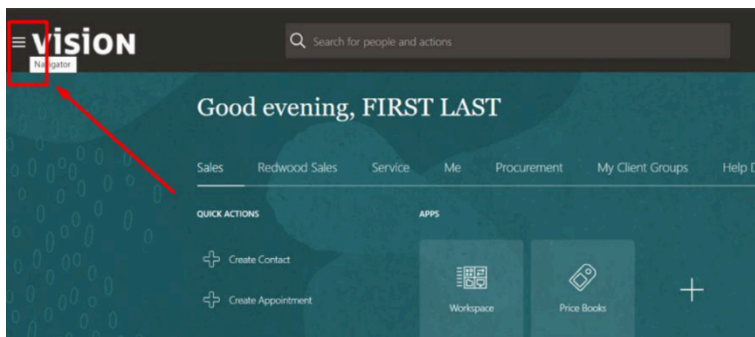


7 Working in AI Agent Studio Data Sources

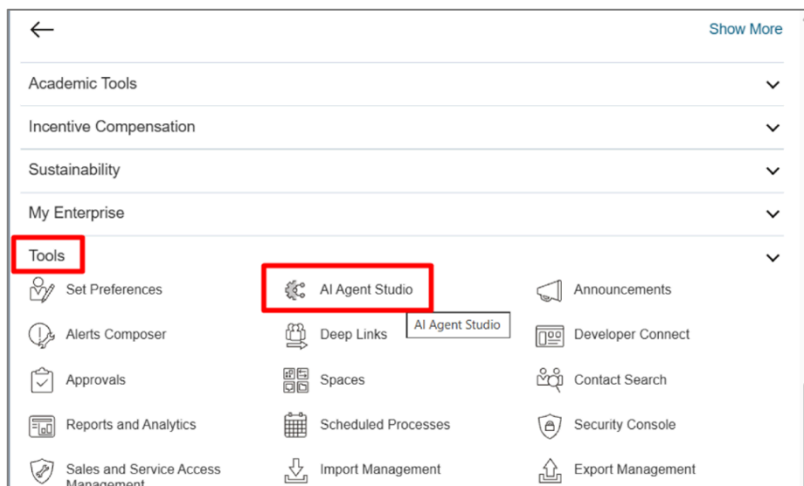
Creating the AI Agent Studio Data Source

Configure Agent Team in AI Agent Studio using the OTM confidential application. There should only be one data source per OTM instance for each release.

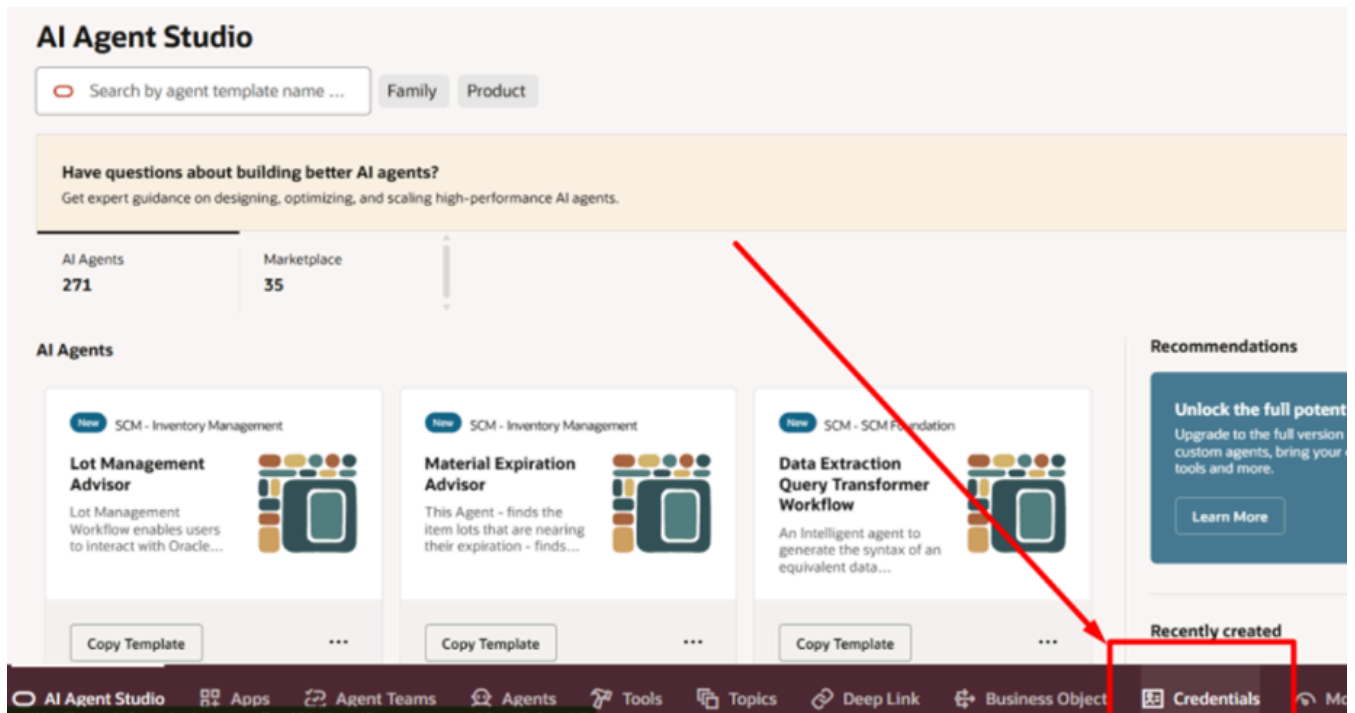
1. Sign in **AI Agent Studio** as an **admin user**.
2. Open the **Navigator**.



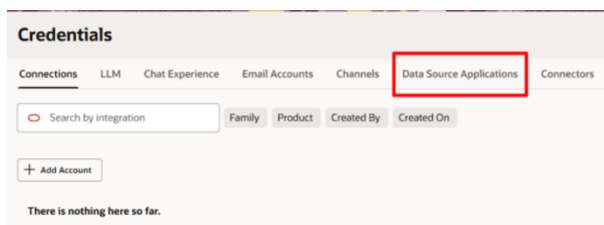
3. Go to **Tools > AI Agent Studio**.



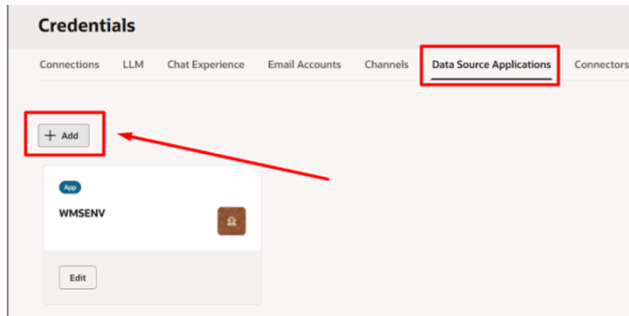
4. Select the **Credentials** tab.



5. Select the **Data Source Applications** tab.



6. Select **+ Add**.



7. Create or edit an entry with a data source **Name** of **OTMENV**.
8. In the **Base Url** field, enter the **OTM Base URL**.
9. In the **IDCS Uri** field, enter the **OTM IDCS URL**.
10. Copy the **Client ID** from the confidential app on IDCS of OTM created previously.
 - | **Note:** Use the value that you wrote down for the **IDCS of OTM confidential app Client ID** in *Prerequisites*.
11. Copy the **Scope** from the confidential app on IDCS of OTM created previously.
 - | **Note:** Use the value that you wrote down for the **IDCS of OTM confidential app Scope** in *Prerequisites*.
12. Enter the **Public Key** created previously. This should be `jwt-signing.crt`.
 - | **Note:** You must paste the CERTIFICATE in this field. Paste the contents of the file including the header and footer sections.
 - | **Note:** Import the certificate that you created earlier. *Generating Public/Private Keys with a Certificate*

13. Enter the **Private Key** created previously. This should be `jwt-signing.key`.

Note: You must paste the private key in this field. Paste the contents of the file including the header and footer sections.

Note: Import the private key that you created earlier. *Generating Public/Private Keys with a Certificate*

Add new data source application details

Name **OTMENV** Required

Base Url **https://[your OTM base URL].oraclecloud.com** Required

IDCS Uri **https://idcs[your IDCS OTM URL].identity.oraclecloud.com/oauth2/** Required

Client Id **The Client ID from the IDCS of OTM confidential app** Required

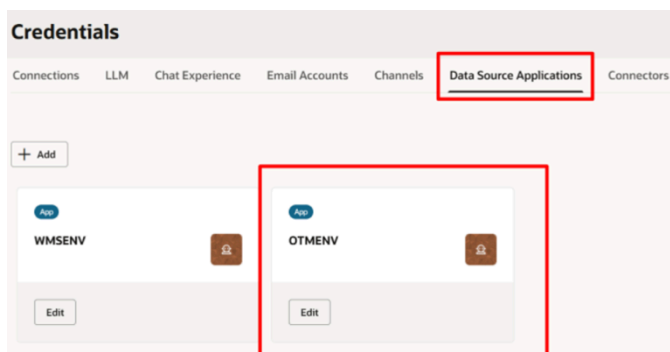
Scope **This is the scope on the IDCS of OTM confidential app.** Required

Public Key **jwt-signing.crt** Required

Private Key **jwt-signing.key** Required

14. Select **Done**.

You see the new **OTMENV** on the Data Source Applications tab.



8 Working in OTM

Setting up AI Agentic Trusts

1. Sign in to **Oracle Transportation and Global Trade Management** as **DBA.ADMIN**.
2. Navigate to **Configuration and Administration > Power Data > AI > AI Agentic Trusts**.
3. Search for and edit the **AI Fusion** record.

AI Agentic Trust		Total Found: 1		
<input checked="" type="checkbox"/>	★	ID	Reserved	Domain Nam
<input type="checkbox"/>	☆	ALFUSION		PUBLIC

4. For the **IDCS Open Authorization URL**, enter the **Fusion IDCS URL**. This should be the Fusion IDCS Auth Token URL.
5. For the **Signing Algorithm**, select **RS256**.
6. For the **Scope**, enter the IDCS of Fusion confidential app **Scope**.
 - Note:** Use the value that you wrote down for the **IDCS of Fusion confidential app Scope** in *Prerequisites*.
7. For **Signing Private Key**, enter `jwt-signing.key`.
 - Note:** Import the certificate that you created earlier. *Generating Public/Private Keys with a Certificate*
8. For **Signing Certificate**, paste the contents of the file `jwt-signing.crt`.
 - Note:** Open the certificate that was created earlier. Copy the contents of the file including the empty line at the end of the file and paste it here.
 - Note:** Import the certificate that you created earlier. *Generating Public/Private Keys with a Certificate*
9. For the **Client ID**, enter the client ID from Fusion IDCS confidential app created previously. This is the unique identifier of the confidential application in the Fusion IDCS domain.
 - Note:** Use the value that you wrote down for the **IDCS of Fusion confidential app Client ID** in *Prerequisites*.

- For the **Client Key ID** enter the **Alias** of the certificate that you imported against the confidential app IDCS of Fusion.

Note: Use the value that you wrote down for the **IDCS of Fusion confidential app certificate Alias** in *Prerequisites*.

- Select **Finished** to save the record.

Adding Access Control Lists to Users

If your OTM users need to use the AI Agents from the AI Chat in OTM.

Note: You must be logged into OTM as the DBA.ADMIN or equivalent user to make these changes.

You need to add a few Access Control Lists to each user as follows:

- In OTM, go to **Configuration and Administration > User Management > User Manager**.
- Search for and edit a user.
- To add access to the Planning Diagnostic AI Agent in AI Chat, search for and add the following access control:
 - REST – Planning Diagnostics**
- Select **Granted**.
- Select **Save**.
- To add access to the Rate Inquiry AI Agent in AI Chat, search for and add the following access controls:
 - REST – Item – View**
 - REST – Location – View**
 - REST – RIQ Actions**
- Select **Granted** and then select **Save**.
- Select **Finished** to save the changes to your user.

OTM AI Chat Agents

Several AI Agents are staged in AI Agent Studio. These agents are used by OTM via the AI Chat functionality.

The bulk plan diagnostic agents are:

- BULK PLAN DIAGNOSTIC – FULL SUMMARY**

- **BULK PLAN DIAGNOSTIC – OPEN ENDED**
- **BULK PLAN DIAGNOSTIC – ORDER ERRORS**
- **BULK PLAN DIAGNOSTIC – SUMMARY**

The **RATE INQUIRY** AI agent is also available for use with the AI Chat functionality.

