Oracle Fusion Cloud Transportation and Global Trade Management

AI Guide

Release 26C

Oracle Fusion Cloud Transportation and Global Trade Management
AI Guide

Release 26C

G56415-02

Author: Oracle Transportation and Global Trade Management Product Team

Contents

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, `jwt-signing.crt`	

Field Name	Value
public key For example, `jwt-signing.key`	

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.

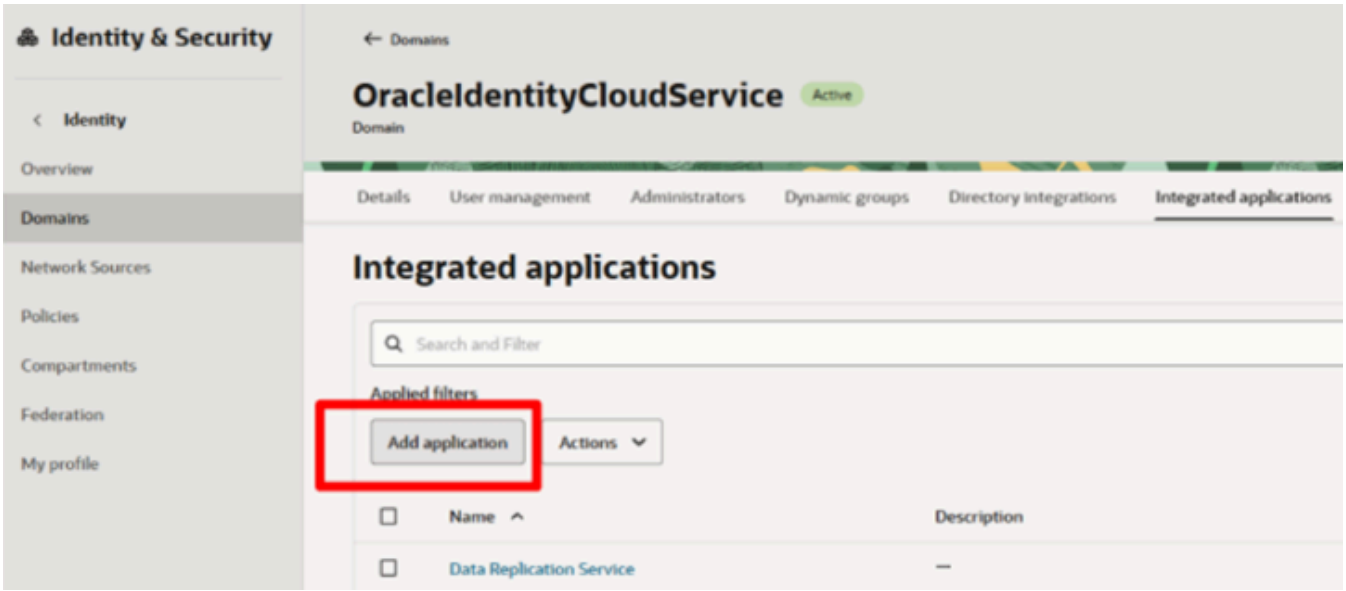
4 Working in OTM IDCS

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.

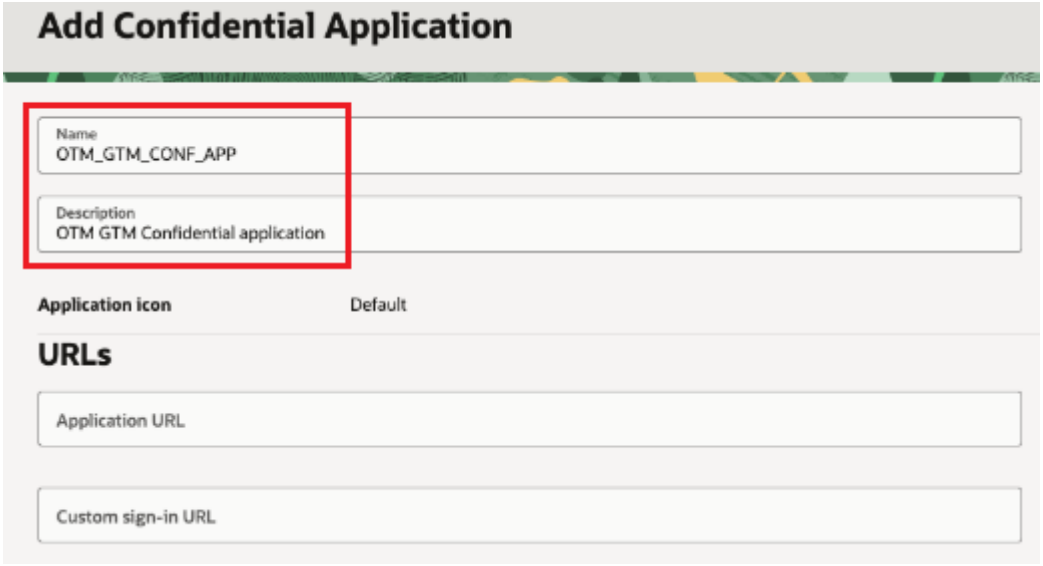
An example of creating the OTM-side confidential application using OTM's IDCS is shown below.

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**.

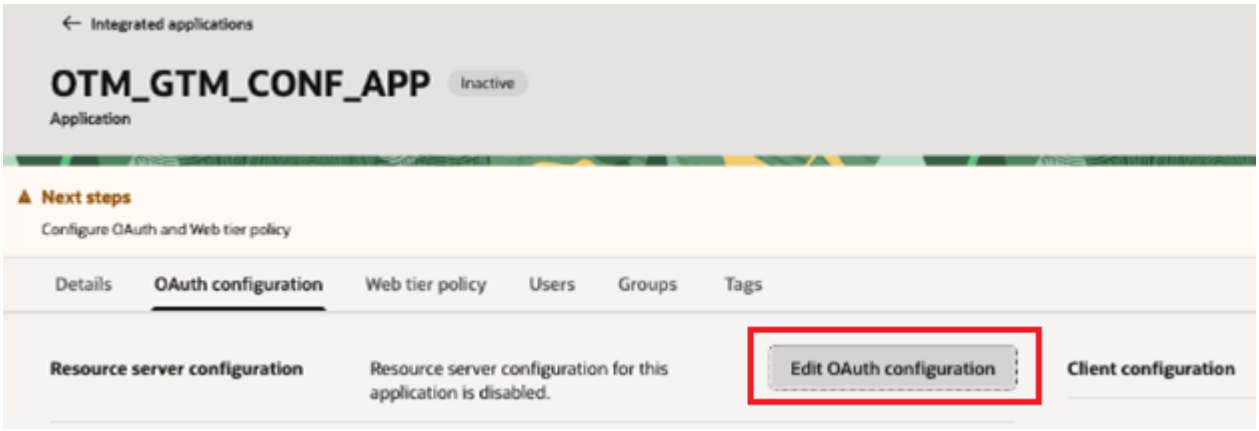


> **Note:** In the *Prerequisites*, write down the **OTM IDCS confidential app Name**. You will need it later.

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

On the new application screen now configure OAuth as follows:

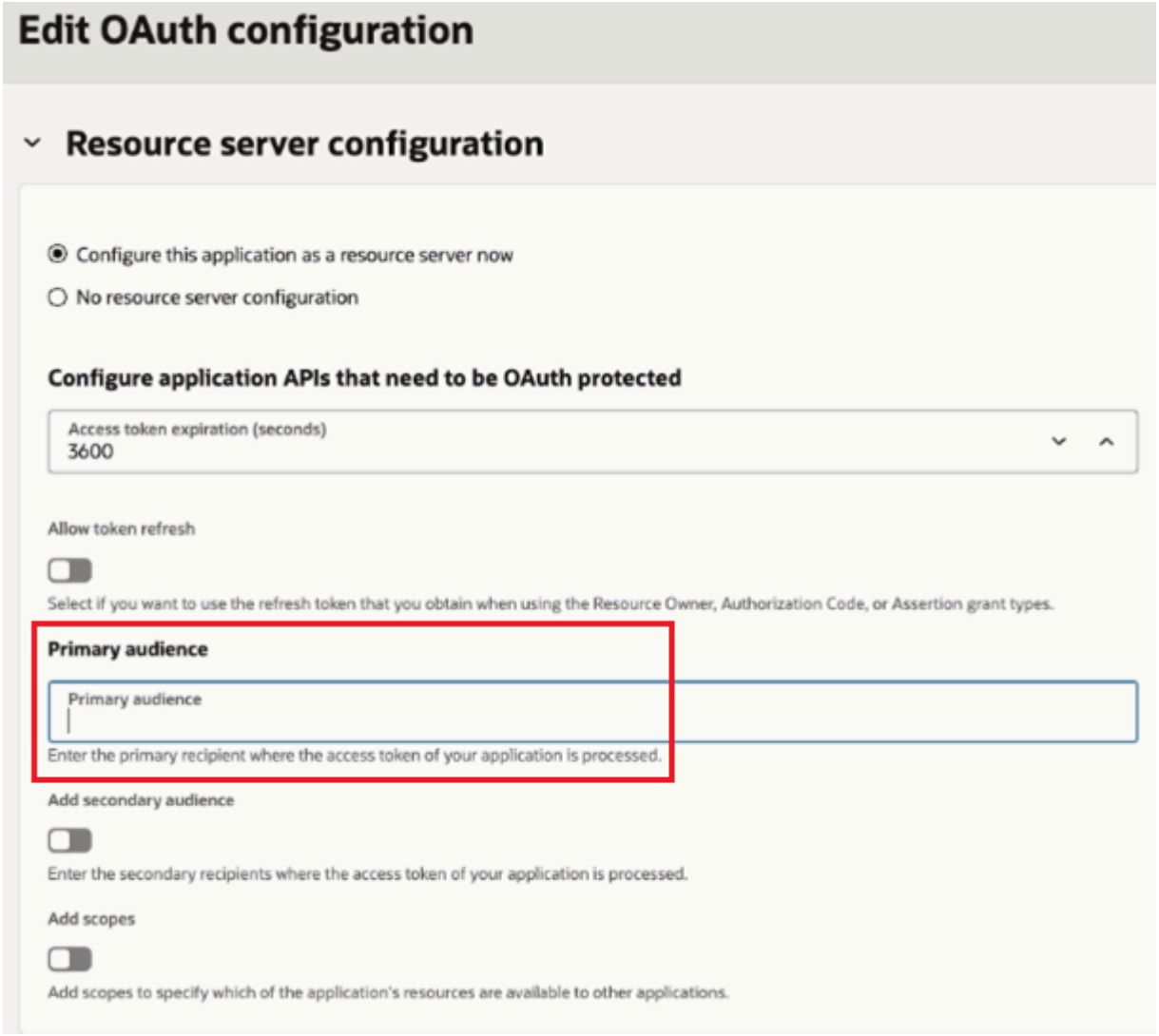
9. Select the **OAuth configuration** tab.
10. Select **Edit OAuth configuration**.



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>`).

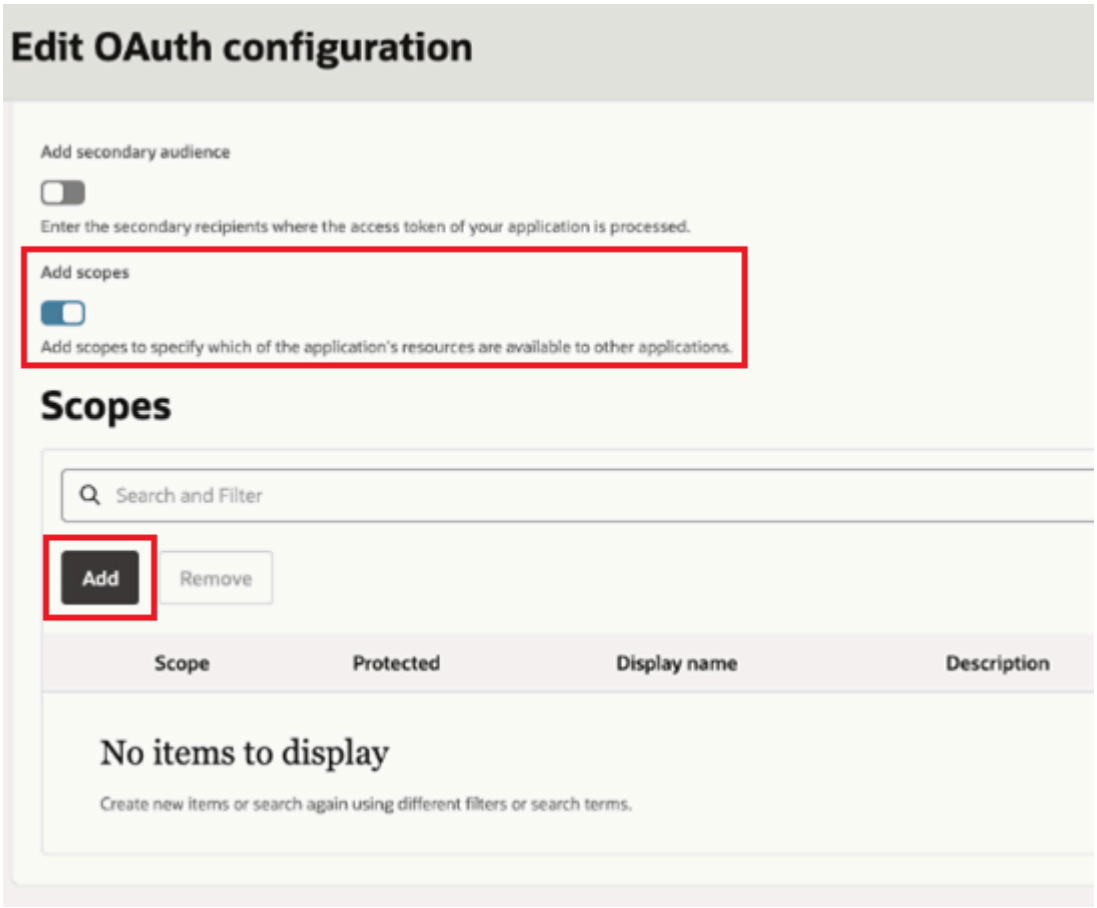


> **Note:** In the *Prerequisites*, write down the **IDCS of OTM confidential app Primary audience** which is the URL of your OTM instance. You will need this later.

Next, you add a scope.

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

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



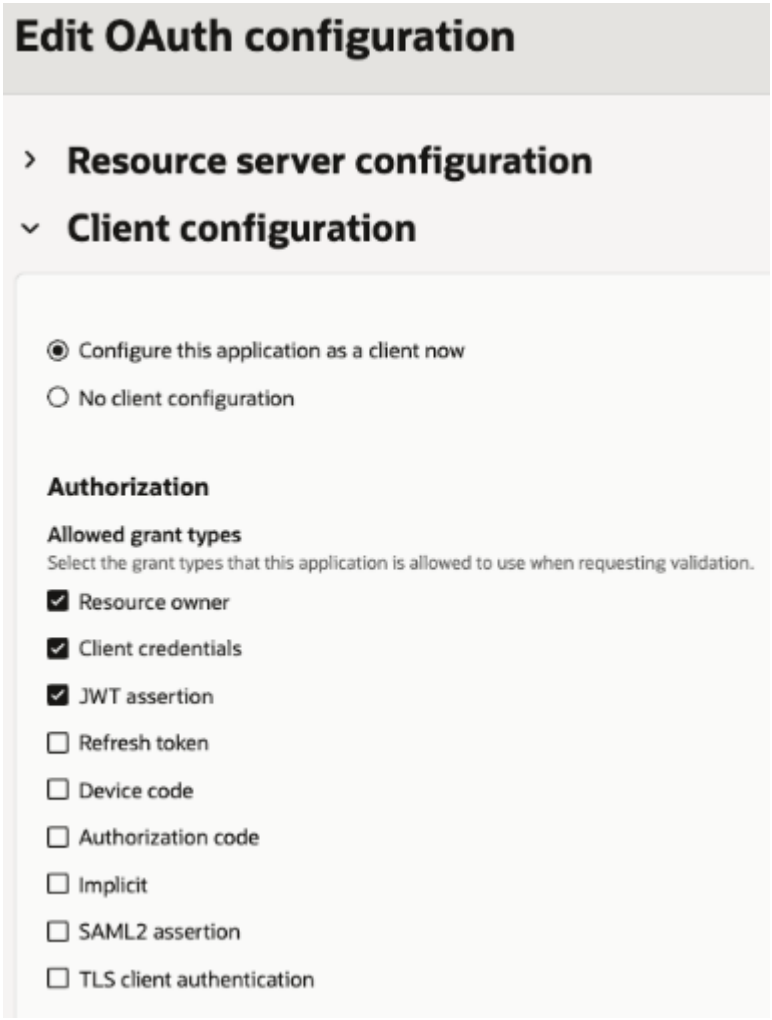
15. Add a **Scope** (for example, `OTM_GTM_CONF_APP`) and a **Description**.

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

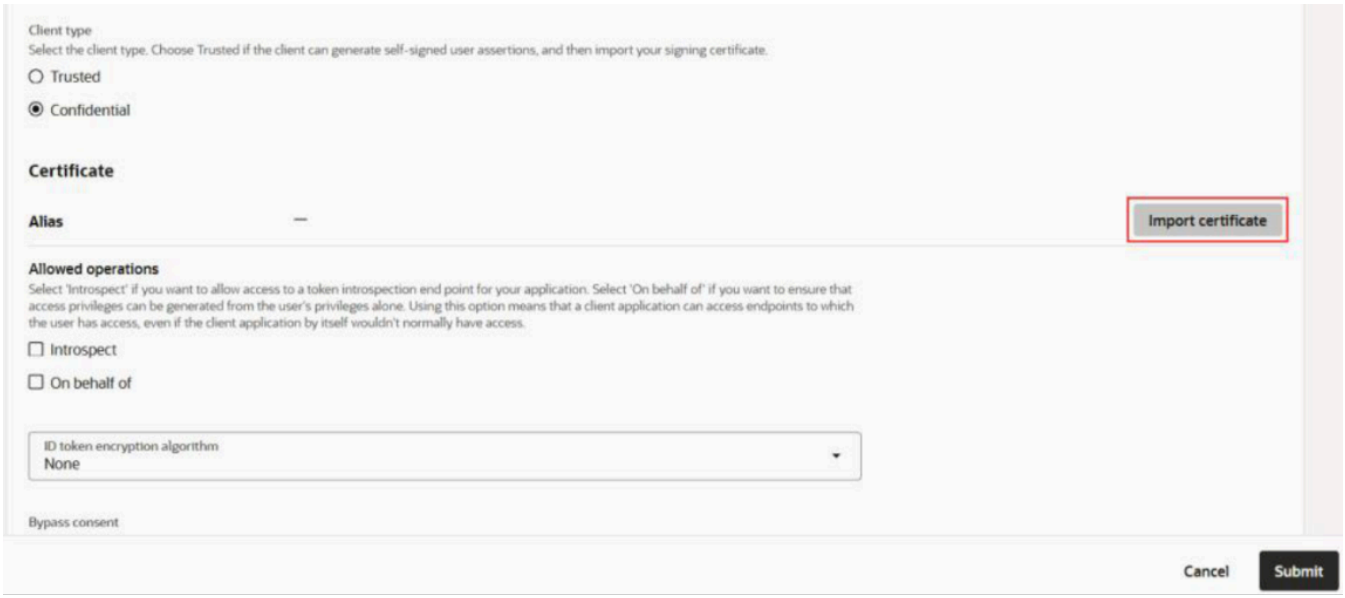
16. Select **Add**.

    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**.



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



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

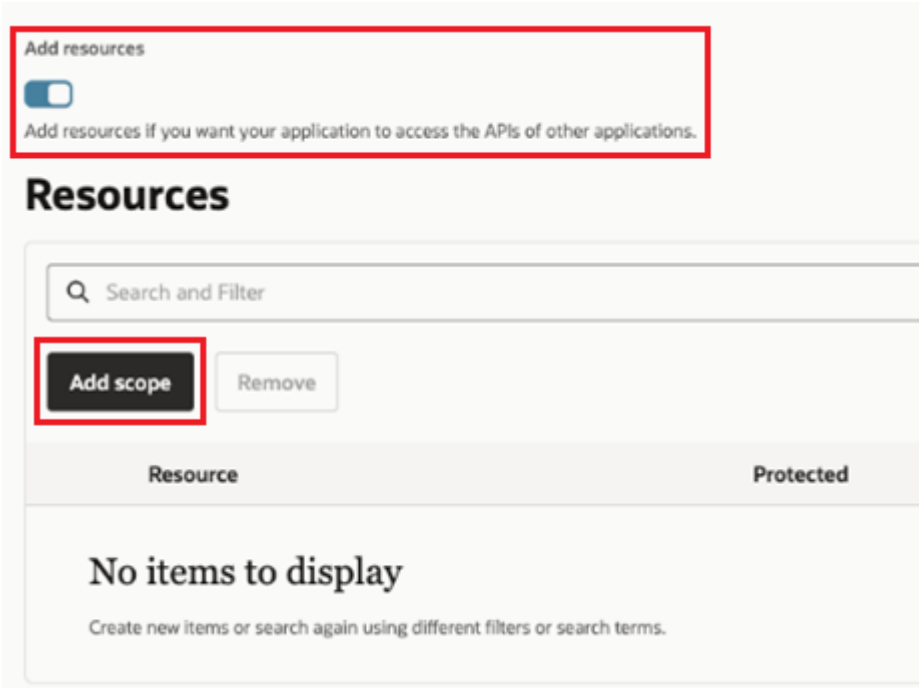
> **Note:** In the *Prerequisites*, write down the **IDCS of OTM confidential certificate Alias**. You will need this later.

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**.

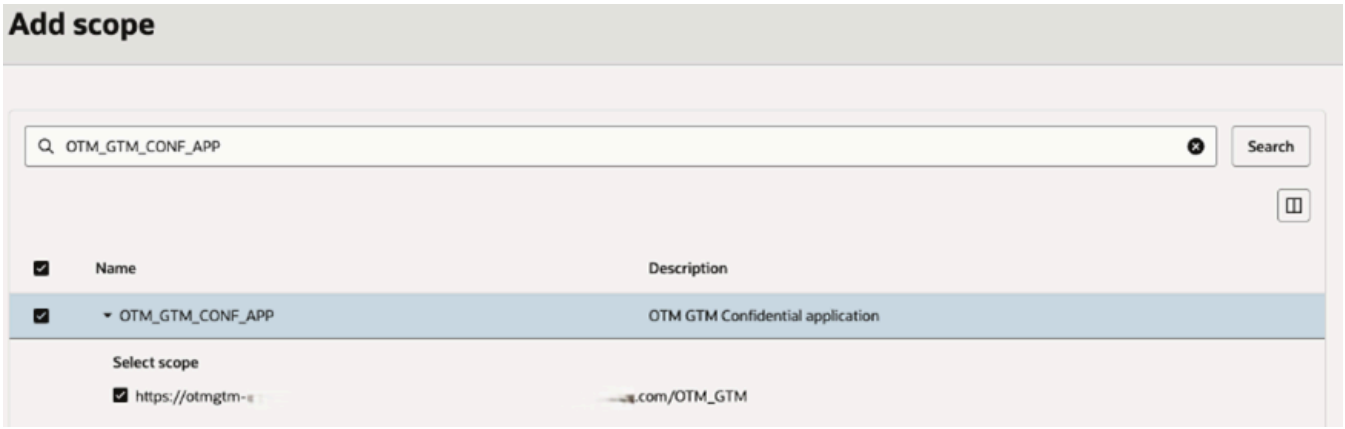
25. Scroll down and select **Add resources**.
26. Select **Add scope**.



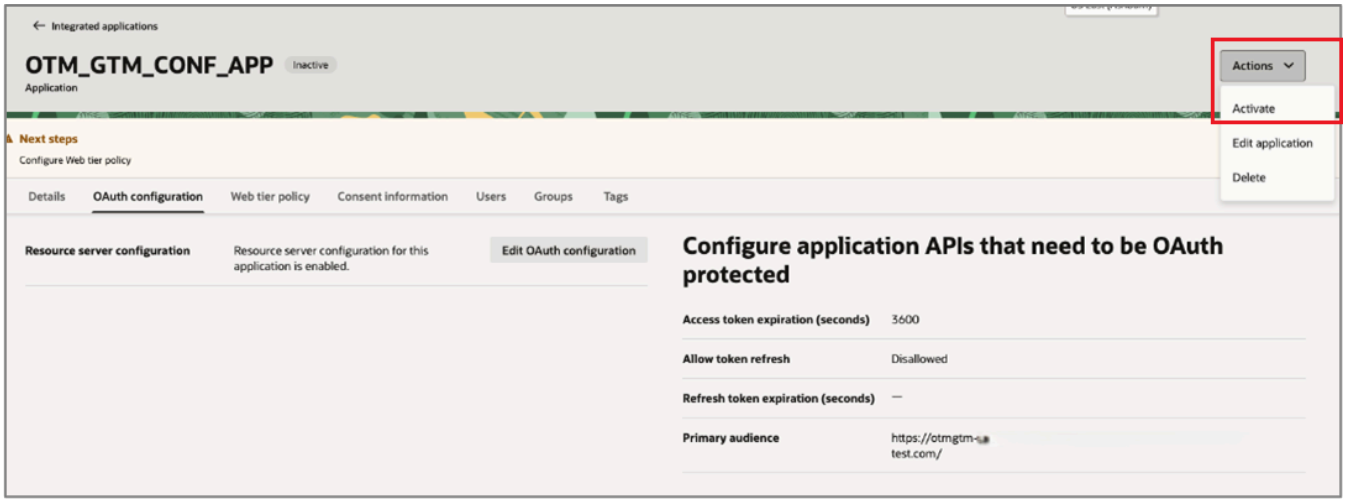
27. Under **Add scope**, select the **Scope** created previously.

> **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**.



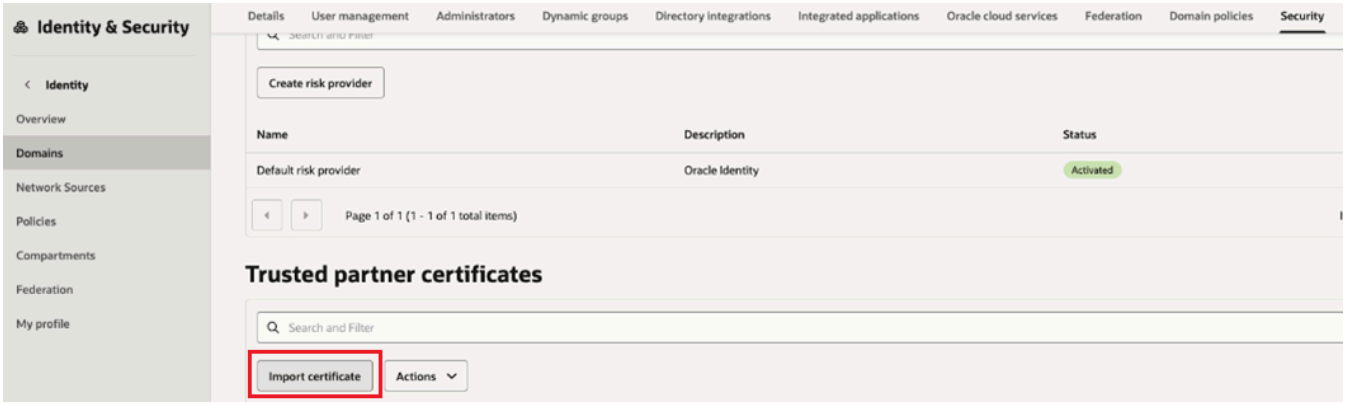
31. On the Activate application message, select **Activate application**.

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**.

Adding Users

Your OTM user needs to access AI Agent Studio. So you can create a user in Fusion IDCS identical to the user in OTM IDCS.

The **username**s field on Fusion IDCS and OTM IDCS must match with the **Nickname** field on the OTM user manager. Usually, this is an email address, but it can be any other unique string.

All all of the following must match exactly:

- Fusion IDCS username
- OTM IDCS username
- Nickname of the OTM user

5 Adding Users

Adding the Users

To enable the AI Chat functionality for your OTM users, they need access to AI Agent Studio. The AI Agents used OTM and GTM are staged in AI Agent Studio. As a result, your OTM users also need to be users in Fusion IDCS and OTM IDCS.

The **username** field on Fusion IDCS and OTM IDCS must match the **Nickname** field on the OTM user. This Nickname can be an email id or any other unique string, but all of the following must match exactly:

- The user name in Fusion IDCS
- The user name in OTM IDCS
- The nickname of the OTM user

6 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:
    - first name
    - last name
    - user name
    - email ID
    - password (twice)
8. Save the new user.

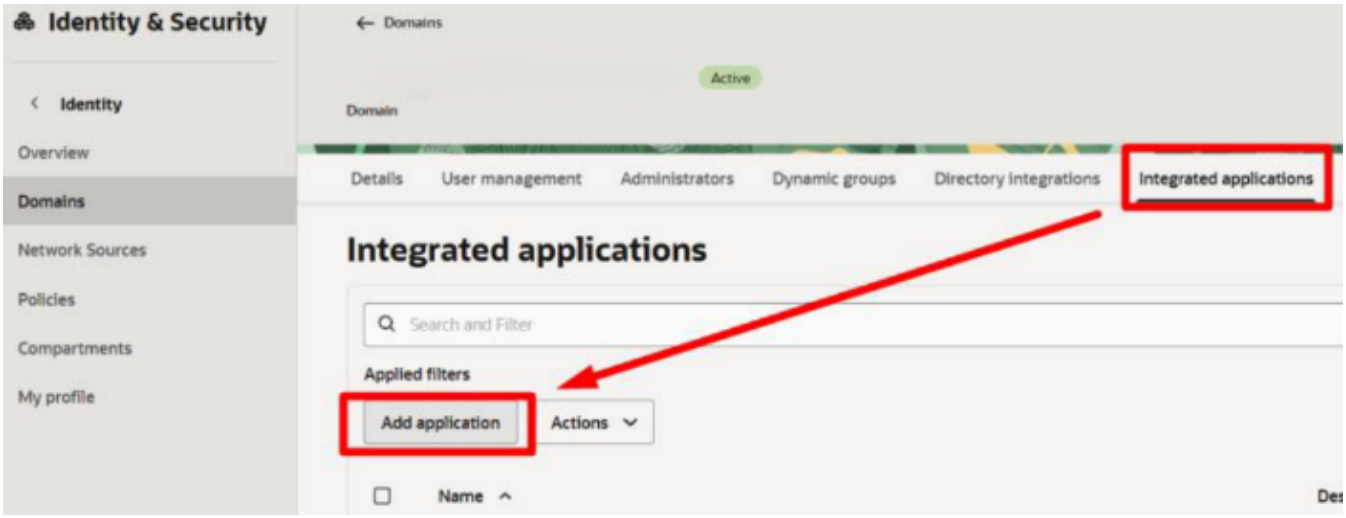
7 Working in Fusion IDCS

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.

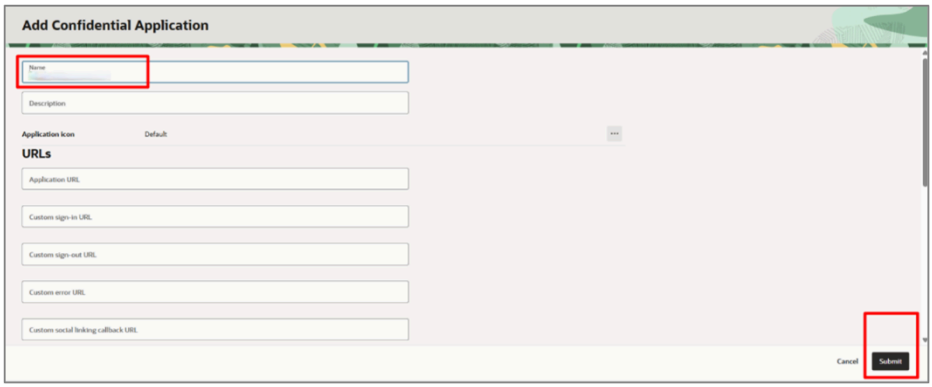
1. Sign in to the **Fusion IDCS Console** as a valid **admin user**.
2. On the **Welcome** page, select **Take me there** to go to the Identity Domain.
3. Navigate to **Identity > Domains**.
4. On the Domain page, select **Integrated applications**. This page is where you'll add an OAuth2 confidential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

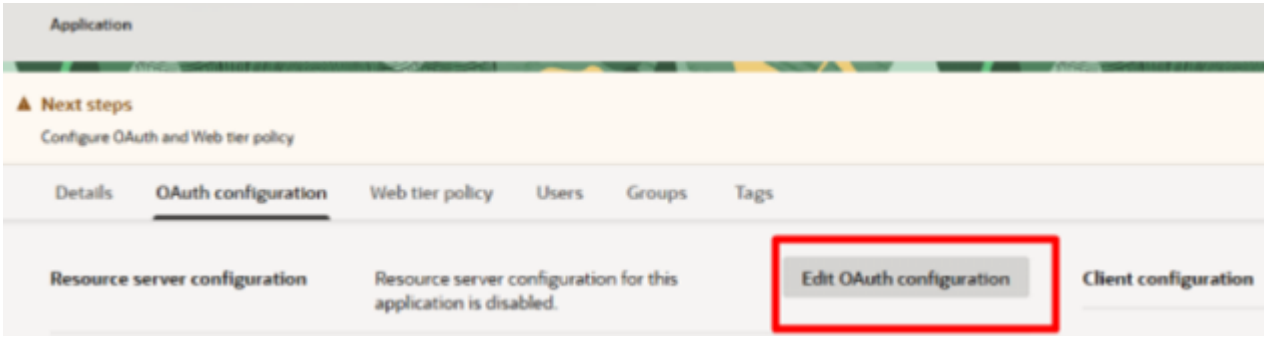
   Note: In the *Prerequisites*, write down the **IDCS of Fusion confidential app Name**. You will need it later.



8. Select **Submit**.

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

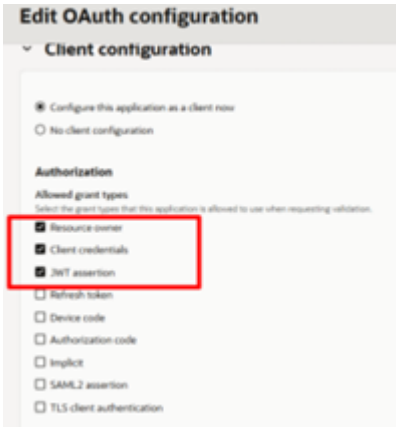
9. Select the **OAuth configuration** tab.
10. Select **Edit OAuth configuration**.



   Next, enable Client Configuration for this OAuth application.

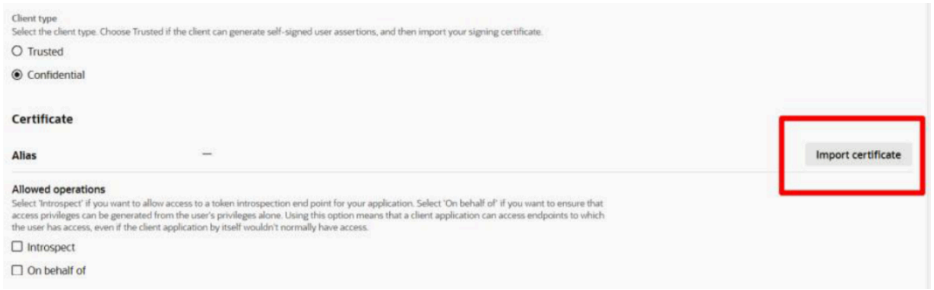
11. Scroll down to the **Client Configuration** section and select the **Configure this application as a client now** option.

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.

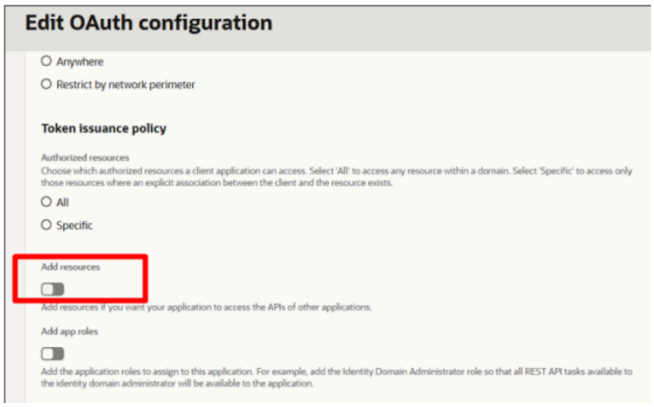
15. Use the **Drop a file or select one** field to upload the certificate. Upload the file `jwt-signing.crt` that was created earlier.

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

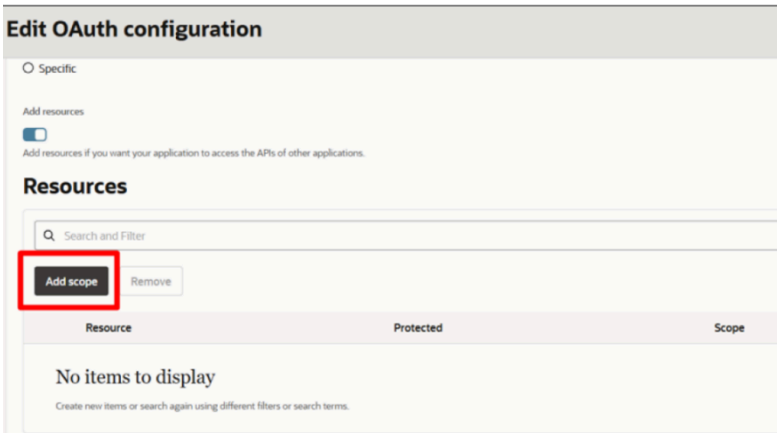
16. Once the certificate is uploaded, select **Import**.

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

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

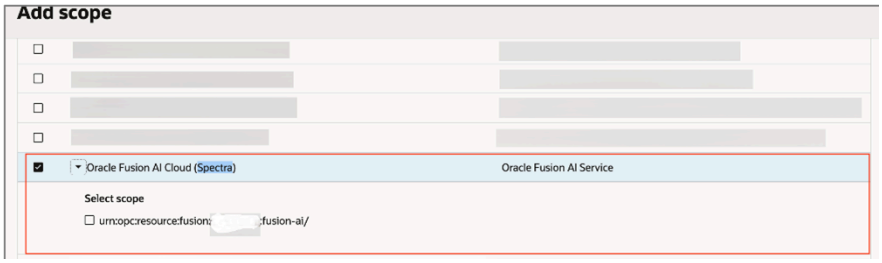


20. Scroll down and select the **Add scope** button.



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

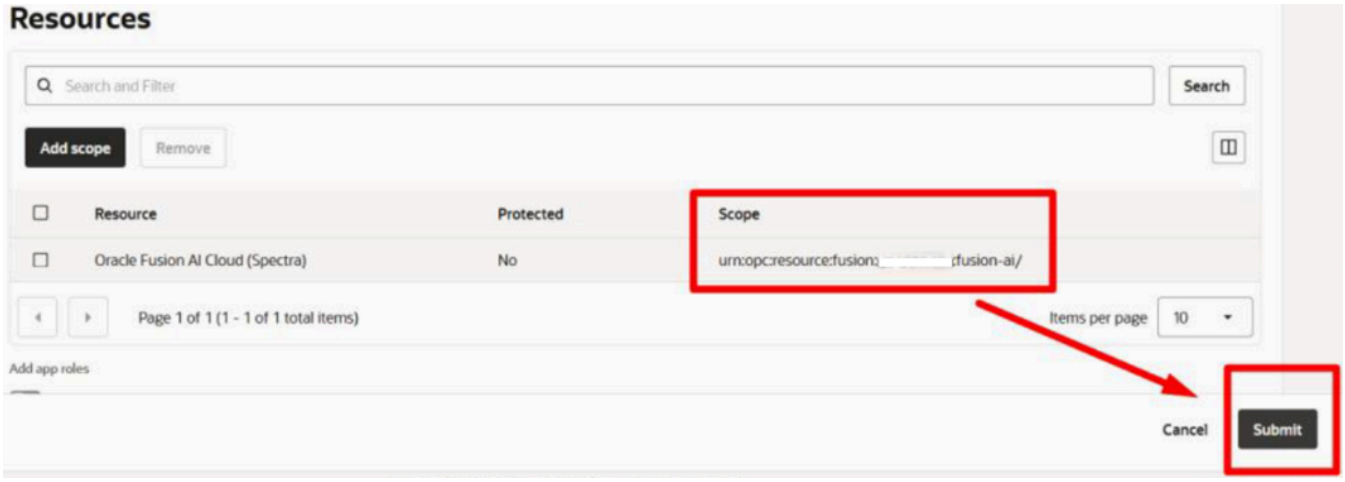
21. Under **Add scope**, select the AI Agent Studio scope with a Name of **Oracle Fusion AI Cloud (Spectra)**.



> **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.

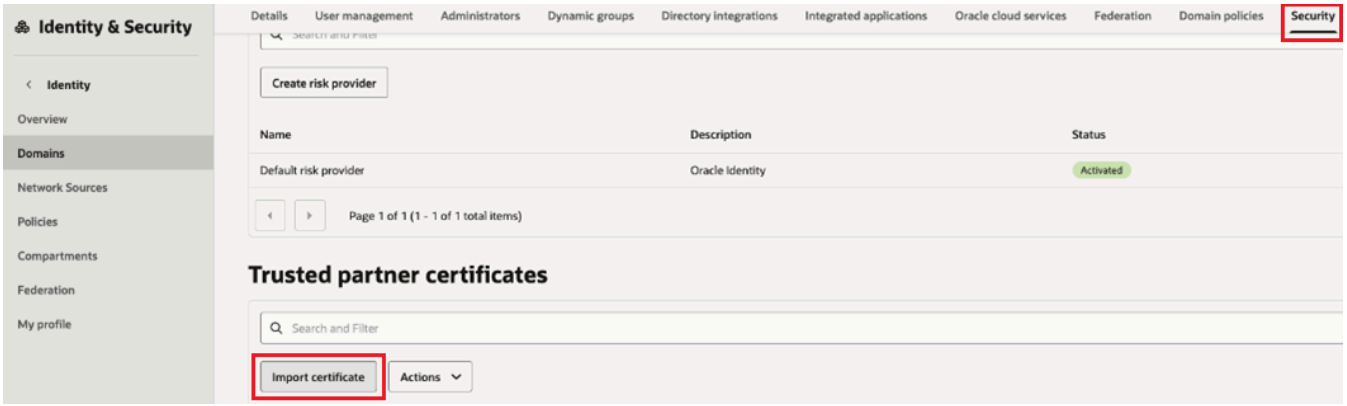
> **Note:** In the *Prerequisites*, write down the **IDCS of OTM confidential app Client ID**. You will need it later.

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*.

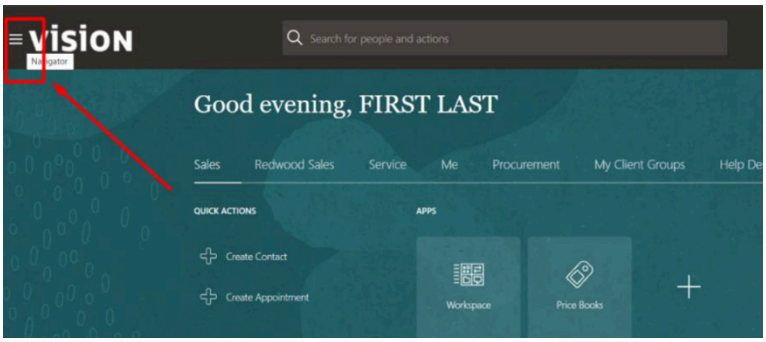
5. Select **Drop a file or select one**.
6. Select the **file used in the previous section**.
7. Select **Import**.

8 Working in AI Agent Studio Data Sources

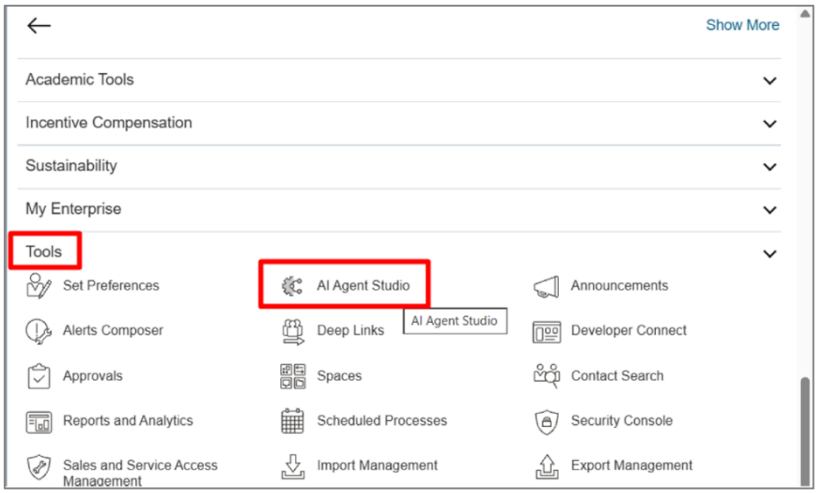
Creating the AI Agent Studio Data Source

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.

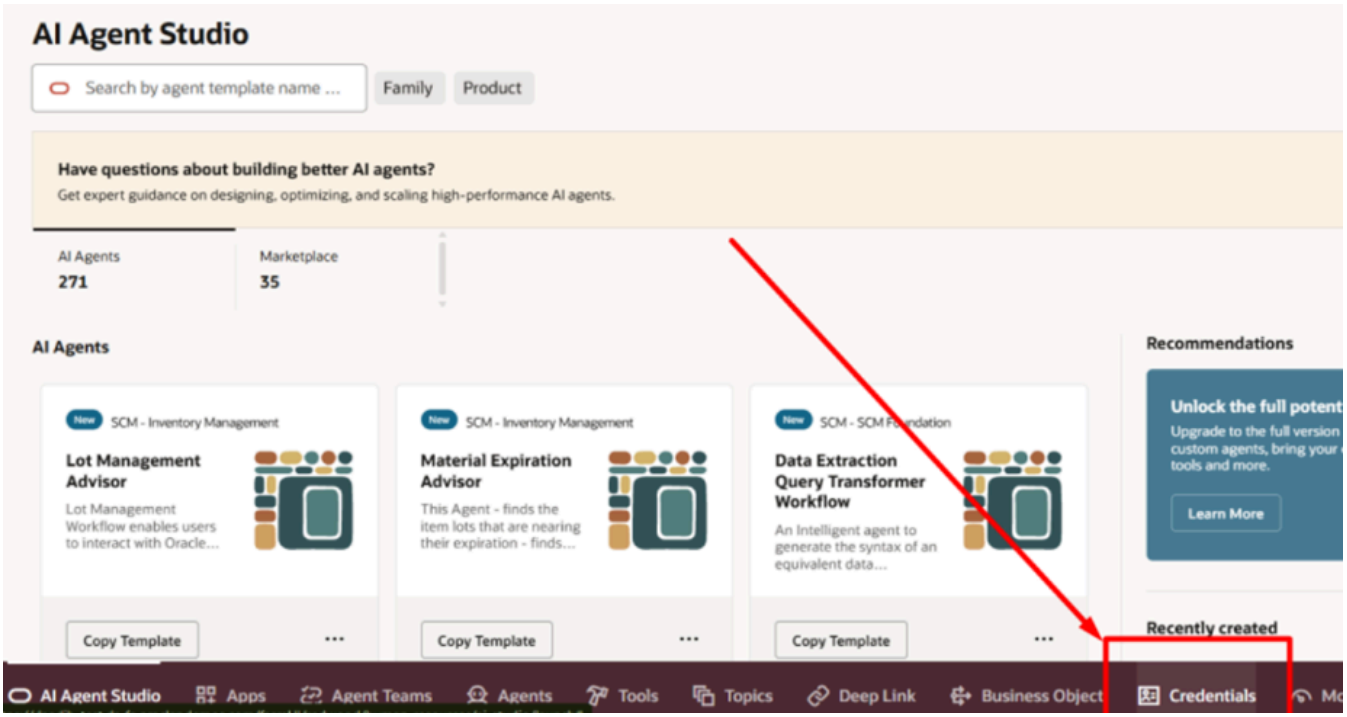
1. Sign in **AI Agent Studio** as an **admin user**.
2. Open the **Navigator**.



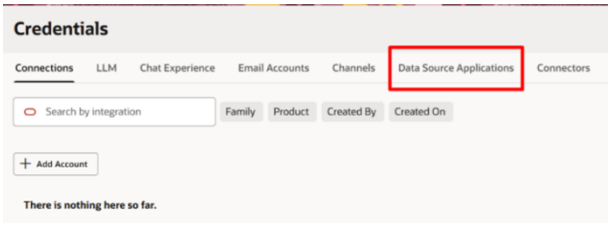
3. Go to **Tools > AI Agent Studio**.



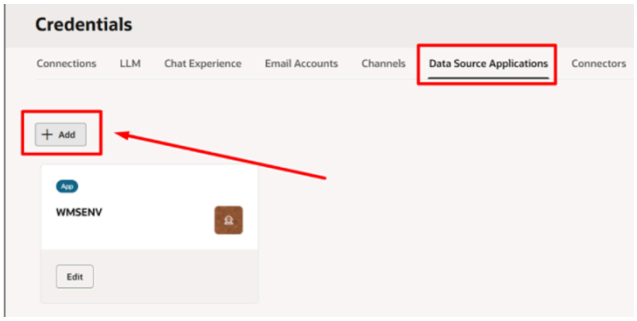
4. Select the **Credentials** tab.



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 Url** 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`.

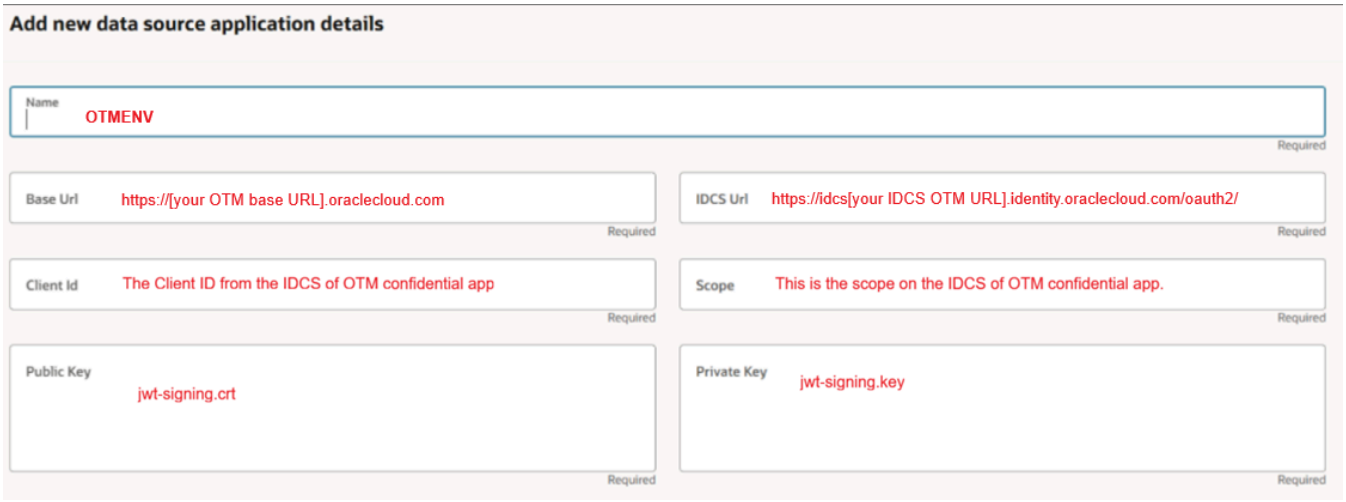
> **Note:** You must paste the CERTIFICATE in this field. Paste the contents of the file including the header and footer sections.

> **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`.

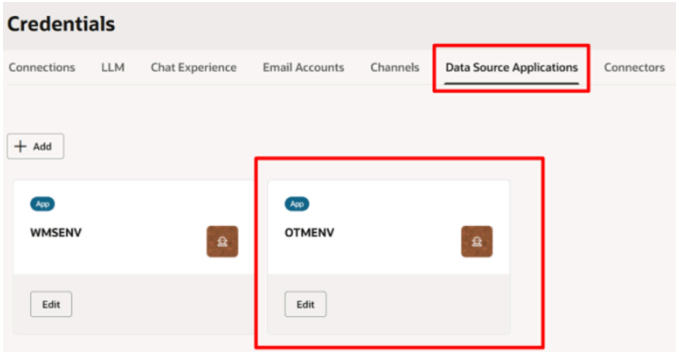
> **Note:** You must paste the private key in this field. Paste the contents of the file including the header and footer sections.

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



14. Select **Done**.

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



Adding the Bulk Plan Tuning Guide to the RAG Tool

Configuring the Diagnostic Agent RAG Tool

1. Download the OTM Bulk Plan Tuning Guide from the Oracle Help Center.

   Then, you edit the tool in AI Agent Studio.
2. Go to the **Tools** tab.
3. Search for the **OTM Bulk Plan Tuning Guide Tool**.
4. Select the **Edit** icon.
5. Under **Documents**, select **+Add**.
6. Enter a **Name** and **Description**.
7. Drag and drop the **Bulk Plan Tuning Guide.pdf** to add it.
8. Change the **Status** to **Ready to publish**.
9. Save/Update the tool.

   Next, you schedule the data ingestion job.
10. Go to **Navigator > Tools > Scheduled Processes**.
11. Select **Schedule New Process**.
12. Enter **Process Agent Documents** in the Name field and wait until Process Agent Documents displays then select it.
13. Select **OK**.
14. On the **Process Details** page, select the **Submit** button.
15. Write down the **Process ID**.

    Then, you track the status of the process.
16. In the **Process Details** page, enter the **Process ID**.
17. Select the **Search** button.
18. When the **Status** changes to **Succeeded**, then you can exit the page.

9 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.

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*.

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

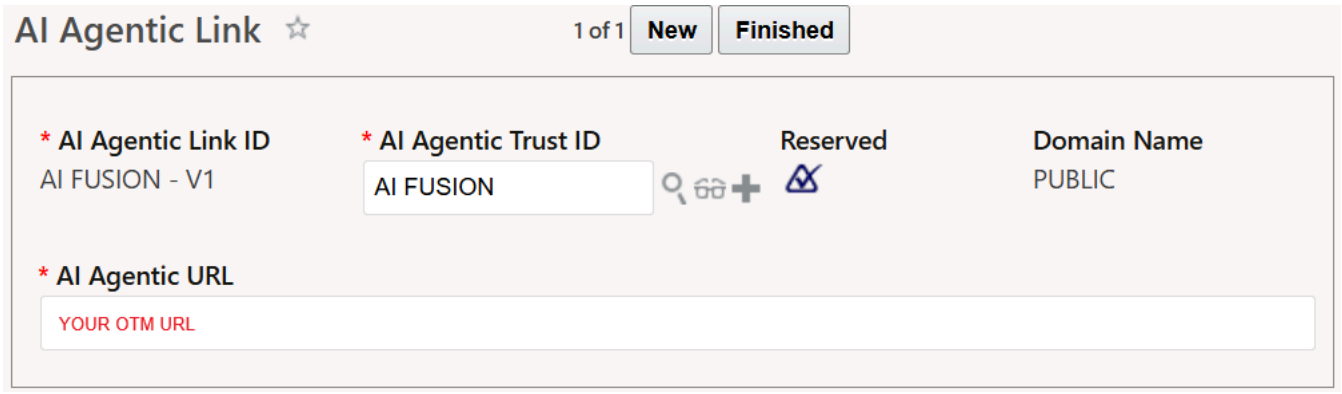
    > **Note:** Use the value that you wrote down for the **IDCS of Fusion confidential app certificate Alias** in *Prerequisites*.

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

Setting up AI Agentic Links

1. Navigate to **Configuration and Administration > Power Data > AI > AI Agentic Link**.
2. Search for an AI Agentic Link ID starting with **AI Fusion**.

   The result will be two records: **AI FUSION - V1** and **AI FUSION -V2**. You will edit both records and specify your OTM URL.
3. Edit **AI FUSION - V1**.
4. For the **AI Agentic URL** enter your **OTM URL**.



5. Select **Finished** to save the record.
6. Edit **AI FUSION - V2**.
7. For the **AI Agentic URL** enter your **OTM URL**.
8. 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:

1. In OTM, go to **Configuration and Administration > User Management > User Manager**.
2. Search for and edit a user.
3. To add access to the Planning Diagnostic AI Agent in AI Chat, search for and add the necessary Access Control Lists as shown in the table:

AI Agents and Required Access Control Lists

AI Agent Name	Required Access Control Lists (ACLs)
BULK PLAN DIAGNOSTICS	REST - Planning Diagnostics
DOCK SCHEDULING	REST - Appointment - View REST - Appointment - Update REST - Appointment - View REST - Location - View REST - Shipment Actions
GTM RESTRICTED PARTY PREPROCESSING ASSISTANT	
PRODUCT CLASSIFICATION ASSISTANT (GTM)	
RATE INQUIRY	REST - Item - View REST - Location - View REST - RIQ Actions
SHIPMENT CHANGE	REST - Shipment - View REST - Shipment Actions

AI Agent Name	Required Access Control Lists (ACLs)
	REST - Tender Actions REST - Tracking Event Configuration - View

4. Select **Granted** and then select **Save** for each required ACL.
5. Select **Finished** to save the changes to the 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.

- **BULK PLAN DIAGNOSTIC – FULL SUMMARY**
- **BULK PLAN DIAGNOSTIC – OPEN ENDED**
- **BULK PLAN DIAGNOSTIC – ORDER ERRORS**
- **BULK PLAN DIAGNOSTIC – SUMMARY**
- **DOCK SCHEDULING**
- **SHIPMENT CHANGE**
- **RATE INQUIRY**
- **PRODUCT CLASSIFICATION ASSISTANT** (GTM)
- **GTM RESTRICTED PARTY PREPROCESSING ASSISTANT**