Oracle® Financial Crime and Compliance Management Cloud Service

Using Application Security Attributes

Release 26.08.01
G59614-01
August 2026

Oracle Financial Crime and Compliance Management Cloud Service Using Application Security Attributes, Release 26.08.01

G59614-01

Contents

About This Content

Use the Application Security Administration to help Administrators classify users and the data that they are permitted to access.

Audience

This guide is intended for administrator users who are tasked with creating and classifying users.

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.

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

About Application Security Administration

Application Security Administration helps Administrators classify users and the data that they are permitted to access.

Users are mapped to user groups, which must be mapped to specific security attributes, such as Business Domain, Jurisdiction, and Case Type. Users can then perform activities associated with their user group throughout the functional areas in the application.

Administrators use this menu to perform the following tasks:

1. Create business domains.
2. Configuring Jurisdictions.
3. Map user groups to security attributes.

1.1 Security within the Application

Security layers control how users interact with the application. The following table describes the security layers.

Table 1-1 Security Details within the Application

Security Layer Type	Controls	Description
Roles	Access to Features and Functions	User roles are used to identify which features and functions the user can access within the application. For example, Case Analysts can access and take action on cases.
Business Domains	Access to Case and Business Information	You can restrict access along operational business lines and practices, such as Retail Banking. Users can only see cases that are assigned to at least one of the business domains their user group is mapped to. For more information about Business Domains, see Create business domains.
Jurisdictions	Access to Case Information	You can restrict access using geographic locations and legal boundaries. Users can only see cases that belong to the jurisdiction their user group is mapped to. For more information about Jurisdictions, see Configuring Jurisdictions.

Table 1-1 (Cont.) Security Details within the Application

Security Layer Type	Controls	Description
Case Type	Access to Cases in Case Manager	**Note:** Case Types are only applicable if your implementation is using Case Manager. Investigation Hub does not currently support Case Type mapping. You can restrict access to specific types of cases. To view a case, users must be mapped to a user group which has access to view the specific Case Type assigned to the case. For more information about case types, see Configure Case Types

1.2 Access Application Security Attributes

To access the Application Security Attributes, follow these steps:

1. In your web browser, enter the application URL to open the **Oracle Cloud Account Sign In** page.
2. On the sign-in page, enter your username and password to log in to the **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service** home page.

   After you sign in, the **Applications**, **Application Administration**, and **Business Processes** tiles are displayed.
3. Select **Application Administration**. The **Application Administration** page is displayed.
4. Select **Application Security Administration**. The **Application Security Administration** page is displayed.
5. You can perform the following activities using the Application Security UI:
   - Configure Business Domains
   - Configure Jurisdictions
   - Configure Case Types

   > **Note**
   >
   > Case Types are only applicable if your implementation is using Case Manager. Investigation Hub does not currently support Case Type mapping.

   - Map user groups to security attributes.

2

About Business Domains

Business domains are used to classify records of different business types (such as Retail Banking vs. Private Banking) or to restrict access to data (such as sensitive employee data).

Records (such as accounts, customers, and cases) can be linked to a business domain. Administrators map user groups to one or more business domains. Users can access records with any business domains that their user group has been mapped to.

For example, you have defined a business domain as EMP: Employee Information. You assign this business domain to the account and customer records that belong to employees. Only users who are in user groups mapped to the EMP business domain can view these records.

Cases can be linked to one or more business domains. User groups who are mapped to either business domain can view these cases. For example, when multiple Events are correlated to a case, if Event1 has come from Retail and Event 2 has come from Institutional Broker-Dealer, then the case belongs to both business domains. Users in user groups mapped to either business domain can view these cases. The **General** business domain is provided by default with this application.

2.1 Adding Business Domains

You can add Business Domains as needed for your implementation.

1. Expand **Application Security Administration** and then select **Business Domains** page. The **Business Domain List** page is displayed.
2. Click **Add**  . The **Add New Business Domain** window is displayed.
3. Enter the details as mentioned in the following table. Mandatory UI elements are marked with an Asterisk *.

Table 2-1 Fields to Add a New Business Domain and their Descriptions

Field	Description
Business Domain Code*	Enter a unique code for the Business Domain. For example, RET for Retail. This field accepts only alphanumeric and hyphen values. Other special characters are not allowed. This field cannot be edited once the business domain is added.
Business Domain Name*	Enter the Business Domain Name. For example, Retail, Institutional Broker-Dealer. This should be a very high-level form of segregation for different areas. This field accepts only alphanumeric, space, underscore and hyphen values. Other special characters are not allowed.

Table 2-1 (Cont.) Fields to Add a New Business Domain and their Descriptions

Field	Description
Business Domain Priority*	Enter the Business Domain Priority. This should be equal to or greater than 1. Lower numbers are considered to be higher priority. When events belonging to different business domains with different priorities correlate to a case, then the business domain with highest priority will be assigned to the case. When events belonging to different business domains of the same priority correlate to a case, that case will have multiple business domains.
Business Domain Description	Enter the Business Domain Description. This field accepts only alphanumeric, space, underscore and hyphen value. Other special characters are not allowed.

4. Click **Save**. A confirmation message is displayed. The newly added business domain will be added in the Business Domain List.

2.2 Editing Business Domains

You can edit existing business domains as needed for your implementation.

1. Expand **Application Security Administration** and then select **Business Domains** . The **Business Domain List** page is displayed.
2. Select the business domain and click **Edit** . The Edit New Business Domain window is displayed.
3. Modify the details as shown in the Fields to Add a New Business Domain table. You cannot edit the Business Domain Code.
4. Click **Save**. A confirmation message is displayed. The business domain in the Business Domain List will be updated.

3
About Jurisdictions

Jurisdictions are used to classify and restrict data.

Users can only access records or cases associated with jurisdictions associated with their user groups. Jurisdictions divide data based on the following types of boundaries, as designated by the financial institution:

- Geographical: division of data based on geographical boundaries, such as countries, states, and so on.
- Organizational: division of data based on different legal entities that compose the client's business.
- Other: combination of geographic and organizational definitions.

Scenario thresholds can be fine-tuned to run different threshold values depending on the jurisdiction.

The Asia Middle East Africa (AMEA) jurisdiction is provided by default with this application.

3.1 Adding Jurisdictions

You can add new jurisdictions as needed for your implementation.

1. Expand **Application Security Administration** and then select **Jurisdictions** page. The *Jurisdiction List* page is displayed.
2. Click **Add**  . The Add New Jurisdiction window is displayed.
3. Enter the details as described in the following table.

Table 3-1 Fields to Add a New Jurisdiction and their Descriptions

Field	Description
Jurisdiction Code*	Enter a unique Jurisdiction Code. For example, AMEA. This field accepts alphanumeric values and underscore(_). Other special characters are not allowed. This field cannot be edited once the jurisdiction is added.
Jurisdiction Name*	Enter the Jurisdiction Name. For example, Asia Middle East Africa. This field accepts alphanumeric values and underscore(_). Other special characters are not allowed.

Table 3-1 (Cont.) Fields to Add a New Jurisdiction and their Descriptions

Field	Description
Jurisdiction Priority*	Enter the Jurisdiction priority. This should be equal to or greater than 1, and priorities must be unique. Lower numbers are considered to be higher priority. Priority can be used to determine the jurisdiction of a case when multiple events are correlated to a case. Each case can have only one jurisdiction; that is, the jurisdiction with higher priority. For example, if Event1 has come from the EMEA jurisdiction with priority 1 and Event 2 has come from the US jurisdiction with priority 2, then the case belongs to the EMEA jurisdiction.
Jurisdiction Description	Enter the Jurisdiction Description. This field accepts only alphanumeric, space, underscore and hyphen values. Other special characters are not allowed.

4. Click **Save**. A confirmation message is displayed. The newly added jurisdiction will be added in the Jurisdiction List.

3.2 Defining Tasks for Batches

To define tasks, you must configure the batches.

The following table lists the tasks which should be configured.

Table 3-2 Task Details for Defining Batches

Field Name	Description	StartBatch Task	EndBatch Task	Other Task
Task Name	Indicates the task name.	Configure	Configure	Configure
Task Description	Indicates the task description.	Configure	Configure	Configure
Task Type	Indicates the task type.	Pre-Configured	Pre-Configured	Pre-Configured
Batch Service URL	Indicates the batch service URL.	Pre-Configured	Pre-Configured	Pre-Configured
Task Service URL	Indicates the task service URL.	Configure as / StartBatch	Configure as / EndBatch	Configure as / ExecutePipeline

The following table lists the parameter which should be configured.

Table 3-3 Parameter Details for Defining Tasks

Parameter Name	Parameter Value
$GROUPNAME$	This value is obtained from the Batch Configuration.
$DATAORIGIN$	This value is obtained from the Batch Configuration.
$FICMISDATE$	This value is obtained from the Batch Configuration.

Table 3-3 (Cont.) Parameter Details for Defining Tasks

Parameter Name	Parameter Value
$BATCHTYPE$	This value is obtained from the Batch Configuration.
$PREVMISDATE$	This value is obtained from the Batch Configuration.
$BATCHRUNID$	This value is obtained from the Batch Configuration.
$JOBNAME$	You must add this parameter and mention the corresponding job name that you want to execute as part of this task.
component	This is applicable only for the ECM start batch task. For more information, see Starting the AMLtoCaseManagement Batch.
dataorigin	This is applicable only for the ECM start batch task. For more information, see Starting the AMLtoCaseManagement Batch.
sourcebatch	This is applicable only for the ECM start batch task. For more information, see Starting the AMLtoCaseManagement Batch.
currentbatch	This is applicable only for the ECM start batch task. For more information, see Starting the AMLtoCaseManagement Batch.

4

About Case Security Mappings

Use the Security Attributes to map user groups with business domains, jurisdictions, and case types. This determines the access privileges users have and which activities they may perform.

User groups must be mapped with the following attributes:

- Jurisdictions
- Business Domains

> **Note**
>
> If your firm has enabled the Compliance Regulatory Reporting application, you can optionally map user groups to a Report Type, used to access the CRR Report in Case Investigation. CRR Reports can be generated without mapping the Report Type attribute, but cannot be viewed unless a Report Type has been mapped.

> **Note**
>
> If your implementation is using Case Manager, you must also map user groups to a Case Type. Investigation Hub does not currently support Case Type mapping.

Before mapping security attributes, you must complete the following:

1. Create users.
2. Map users to user groups.
3. Create business domains.
4. Create jurisdictions.

4.1 Mapping Security Attributes

You can map user groups to security attributes.

1. Expand **Application Security Administration** and then select **Security Mappings** . The **Security Mappings** page is displayed.
2. Select the User Group that you want to map with the Security Attributes (Jurisdiction, Business Domain, and Case Type) from the **Select User Group** drop-down list.
3. Map one or more Jurisdictions to a User Group by moving the jurisdiction from the **Available Jurisdictions** list to the **Selected Jurisdictions** list. This allows users in this user group to access cases that belong to the mapped jurisdiction.
4. Map one or more Business Domains to a User Group by moving the Business Domain from the **Available Business Domains** list to the **Selected Business Domains** list. This allows users in this user group to access cases that belong to the mapped Business Domain.

a. **Optional**: Map one or more Case Types to a User Group by moving the Case Type from the **Available Case Types** list to the **Selected Case Types** list. This allows users in this user group to access cases that belong to the mapped Case Type.

b. **Optional**: Map one or more Report Types to a User Group. For mapping, move the Report Type from the **Available Report Types** list to the **Selected Report Types** list. This allows users in this user group to access cases that belong to the mapped Report Type.