Oracle® Fusion Middleware

Help Reference for Oracle Advanced Authentication Admin Console

F39316-04
October 2022

Oracle Fusion Middleware Help Reference for Oracle Advanced Authentication Admin Console,

F39316-04

Primary Author: Oracle Corporation

Contents

Preface

1 Oracle Advanced Authentication Home Page

2 Oracle Adaptive Risk Management Home Page

Preface

The Oracle Fusion Middleware Help Reference for Oracle Advanced Authentication introduces you to OAA Admin Console UI.

Audience

This document is intended for Administrators who use the Oracle Advanced Authentication Admin Console.

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 Documents

For more information, see the following documents:

- *Oracle Fusion Middleware Administering OAA and OARM*
- *Oracle Fusion Middleware Administering Oracle Access Management*

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

Oracle Advanced Authentication Home Page

Oracle Advanced Authentication admin console provides options to create and manage agents, assurance levels, and policies for integrating with clients, such as Oracle Access Management (OAM) and Oracle Radius Agent, and implement multi-factor authentication.

Quick Actions

Element	Description
Create Agent	Click **Create Agent** to start creating a new agent for integration with Oracle Advanced Authentication (OAA).
Create OAM Integration	Click **Create OAM Integration** to start creating a new agent for integrating Oracle Access Management (OAM) with OAA.
Create Radius Agent	Click **Create Radius Agent** to start creating a new agent for integrating Oracle Radius Agent client with OAA.
☰	Click ☰ to open or close left navigation window.
?	Click ? and • Click **About** to get more information about Oracle Advanced Authentication (OAA). • Click **Help** to open the Online Help for OAA Admin Console.

Recent Activity

Lists all the Agents that were created newly. To open a complete list of all the Agents created on the OAA admin console, do one of the following:

- Click the **Application Navigation** icon ☰ on top-left and click **Manage Agents**.
- Click **Show more agents** under **Recent Activity**.

1.1 Create Agent

To create an integration between Oracle Access Management (OAM), RADIUS, or a REST-based application with Oracle Advanced Authentication (OAA), you must create and register these agents.

Prerequisite: Before you progress, ensure that you have registered the Client as a TAP partner of OAA and have all the necessary details such as TAP Partner name, Java KeyStore file (.jks), and KeyStore Password available.

For more information about Registering Client as TAP partner, see Register OAA as a TAP Partner in OAM.

Details

Element	Description
Name	Specify the name of the Agent. It must be the same as the partner name created while registering the Client as a TAP partner of OAA.
Description	Provide a clear description about the Agent.
Agent Type	Select the corresponding Agent Type from the drop-down menu: • **OAM**: Choose this if you are integrating OAA with Oracle Access Management (OAM). • **Radius**: Choose this if you are integrating OAA with a Radius Client. • **REST API**: Choose this if you are integrating OAA with a client using REST APIs.
Client ID	Click **Re-Generate** to create a Client ID Click **Copy** to copy the generated Client ID **Note:** This Client ID needs to be provided when configuring the client.
Client Secret	Click **Re-Generate** to create a Client Secret. Click **Copy** to copy the generated Client Secret . **Note:** This Client Secret needs to be provided when configuring the client.
Private Key File	**Drag and Drop** the Java KeyStore file (.jks) that was created after registering the Client as a TAP partner of OAA. For example, `OAMOAAKeyStore.jks`. Alternatively, click **+** to select the file from the file system.

Element	Description
Private key Password	Specify the password that you had provided while registering the Agent as a TAP partner of OAA.
Save	Click **Save** to complete the agent registration with OAA.
Cancel	Click **Cancel** to cancel the changes made to the page.

Assurance Levels

After you **Save** the Agent, click on the **Assurance Levels** tab to create an Assurance level for the Agent

Element	Description
Create	Click **Create** to create an assurance level for the Agent
Delete	If you have not created an assurance level, the Delete button is disabled. After you have created the assurance level, you can choose to delete it by clicking **Delete**.
Name	Lists the Assurance Levels created
Description	Displays description for each of the Assurance Levels.

Groups

After you **Save** the Agent, click on the **Assurance Levels** tab to create an Assurance level for the Agent

Element	Description
Create	Click **Create** to create a group for the Agent
Delete	If you have not created an Group, the Delete button is disabled. After you have created the Group, you can choose to delete it by clicking **Delete**.
Name	Lists the Groups created.
Type	Displays the Group Type.
Description	Displays description for each of the groups.

1.2 Create Assurance Level

Assurance Level indicates the level of assurance that is needed by the agent.

Prerequisite: Ensure you have created the Agent. You can create the assurance level only after you have created the Agent.

Details

Element	Description
Name	Specify a name for the Assurance Level.
Description	Provide a clear description about the Assurance Level.
Create	Click **Create** to create the assurance level for the agent.
Cancel	Click **Cancel** to cancel the changes made to the page.

1.3 Create Group

Group is a collection of similar entities. For example, IP address.

Prerequisite: Ensure you have created the Agent. You can create the Group only after you have created the Agent.

Details

Element	Description
Name	Specify a name for the Group.
Description	Provide a clear description about the Group.
Type	Choose a Group Type from the drop-down menu, based on which the group is created: • **User ID**: Select this option to associate the agent with group based on User Ids. • **IPs**: Select this option to associate the agent with group based on specific IP address. • **IP Ranges**: Select this option to associate the agent with group based on IP address in the specified range. • **Generic Strings**: Select this option to associate the agent with group based on the specified string.
Create	Click **Create** to create the Group for the agent.
Cancel	Click **Cancel** to cancel the changes made to the page.

Values

Element	Description
Add	Click **Add** to add values for the group based on its group type.
Delete	Click **Delete** to delete a value from the list.
Value	Lists all the values that you have created for the group.

Add Value

Element	Description
Values	Based on the Group Type you had selected, specify the corresponding values. • For **User ID** type, specify the user IDs • For **IP** type, specify the IP address • For **IP Ranges** type, specify the IP range in the following fields: – **Name**: Specify a name. – **Description**: Add a description. – **From**: Specify the starting IP address of the range. – **To**: Specify the ending IP address of the range. • For **Generic Strings** type, specify the corresponding string.
Save	Click **Save** to save the values for the group.
Cancel	Click **Cancel** to cancel the changes made to the page.

1.4 Define Policy

Define Policy window enables you to create rules by setting conditions, against which the selected challenge factors need to be applied.

Basic

Element	Description
Use the Factor (s)	Select any or all of following challenge factors that need to be applied: • Oracle Mobile Authenticator • Email Challenge • Yubico OTP Challenge • SMS Challenge • FIDO2 Challenge

Element	Description
If the following condition(s) are met	Set the conditions by creating expressions using Attribute, Operator, and Values/Groups. The Challenge Factors are applied based on this condition. • **Attribute Name**: Select an attribute from the drop-down list. • **Operator**: Select one of the following conditional operator from the drop-down. – In Range – Not In Range – Equals – Ends with – Not Equals – Not in Group – In Group – Begins with • **Value/Group**: Select the corresponding value or group, based on the attribute and the operator selected.
+	Click to add a new policy for the Agent. You can add multiple policies for the Agent
+	Click to add new condition. You can add multiple conditions to the policy.
Validate Rule	Click **Validate** to verify the correctness of the condition set.

1.5 Agents

The Agents window lists all the Agents created in Oracle Advanced Authentication (OAA) Admin Console.

To open the Agents list window, do one of the following in the Home Page:

- Click the **Application Navigation** icon on top-left and click **Manage Agents**.
- Click **Show more agents** under **Recent Activity**.

Element	Description
Create	You can create a new Agent by clicking **Create**.
Delete	To delete an agent from the list, select the check-box against the Agent Name that you need to delete, and click **Delete**. To delete all Agents listed, click the check-box at the top head row and click **Delete**.
Name	Displays the name of the Agent. You can sort the Agent list in Alphabetical Ascending or Descending order.
Description	Displays the description that you had provided against each of the Agents listed.

Element	Description
Client ID	Displays the Client ID for each of the Agent that you had generated on the Create Agent window.
Agent Type	Displays the Agent type against each of the Agent name: **oam**, **api**, or **radius**.

1.6 Groups

Lists all the Groups created for the agent and its corresponding assurance level in Oracle Advanced Authentication (OAA) Admin Console.

To open the Groups list, perform the following steps:

1. Click the **Application Navigation** icon on top-left and click **Manage Agents**.
2. From **Agents** window, click on the required agent name.
3. Click the **Groups** tab to open the groups list.

Element	Description
Name	Displays the name of the Group.
Type	Displays the group type against each of the group name: **User ID**, **IPs**, **IP Ranges** or **Generic Strings**.
Description	Displays the description that you had provided, against each of the group names.

1.7 Assurance Levels

Lists all the Assurance Levels created for the Agent.

To open the Assurance Level list, perform the following steps:

1. Click the **Application Navigation** icon on top-left and click **Manage Agents**.
2. From **Agents** window, click on the required agent name.

Element	Description
Name	Displays the name of the Assurance Level.
Description	Displays the description that you had provided, against each of the Assurance Level names.

2 Oracle Adaptive Risk Management Home Page

OARM provides a streamlined and a robust interface for administrators and analysts. Administrators can easily identify access requests and monitor alerts to uncover fraud and misuse.

Monitored User Activities

User Activity is an operation performed by the user that requires monitoring. For instance, logging in, user transaction's like retail banking, credit card based activity, and so on.

Element	Description
User Authentication	Out-of-the-box, OARM provides an user activity called **User Authentication**, which is built with a rich set of prepacked rules. User Authentication activity evaluates user activities to detect threats and takes remedial actions and raise alerts.
Create Custom Activity	A customer can create their own custom activities in addition to the out-of-the-box **User Authentication** activity and create rules using the information collected from this custom activity. Rules are customized according to the business needs. These can be transactional in nature, monitoring various aspects of the user activity that the business is interested in.

2.1 Add New Rule

Rules are a collection of conditions used to evaluate user activity. Rules are also used to make decisions like alerting an administrator or next action to be taken based on the outcome.

OARM provides out-of-the-box rules that address basic registration and authentication flows in OARM. You can also create your own rules to support the required business logic.

Add New Rule

To create a rule, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Adaptive Risk Management**.
2. From the **User Authentication** tile, click the **Rules** link.
3. Click **Add New Rule**.

Elements	Description
Name	Specify a name for the rule.

Elements	Description
Status	This option specifies to activate the rule. If you want the rule to function as soon as it is created, keep the default, `Active`, for the **Status**.
Description	Specify a description for the rule.
Select Action	From the **Select Action** group list, select the action you want triggered by this rule.
Select Alert	From the **Select Alert** group list, select the alert you want to send if this rule is triggered.
Search Condition	From the **Search Condition** list, select the condition that you want to associate with the rule, and click **Add Condition**. The parameters of the condition are displayed at the bottom of the page, which you can modify as per your requirement, and then click **Save**.
Show Advanced Conditions	Use this toggle button to view the list of advanced conditions, which are added in the **Search Condition** list.

2.2 Create Custom Activity

In addition to the out-of-the-box User Authentication, you can create your own user activity, which is known as the Custom Activity. You can create rules customized to your business needs.

You can create a custom activity using either of the following methods.

Method 1

To create a custom activity, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Adaptive Risk Management**.
2. On the **Monitored User Activities** page, click **Create Custom Activity**.
3. On the **What is a Custom Activity** page, click **Create Custom Activity**.

Method 2

To create a custom activity, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Custom Activities**.
2. Click **Create**.

Describe Activity

Elements	Description
Enter a name for this Activity	Specify a unique name for the custom activity.
Description	Specify a description for the custom activity.

Create New Actor

An actor is a data structure that you can reuse in multiple custom activities. For example, an address actor could be used as a shipping address, billing address, home address, and so on.

To add an actor to a custom activity, click **Next**, and then do one of the following:

- Click **Select an Actor** to add an existing actor provided out-of-the-box.
- Click **Create New Actor**.

Select an Actor

Elements	Description
Select	Select an actor provided out-of-the-box. You now need to provide the following details for the selected actor: • **Source Data:** It refers to client data that is coming from a protected application as part of a transaction. For example, `src.country`. • **Mapping Type:** Mapping is a way to connect the source data to destination data and to actor. Select the mapping type as follows: – Select `Direct` if you want a one-to-one mapping of the source data element to the destination data element.
Provide instance name for this actor	Specify the name of the instance for the actor.

Create New Actor

Elements	Description
Name	Specify a unique name of the actor. For example, for the Address actor, enter `Address` in the **Name** field.
Description	Specify the description of the actor. For example, you can enter `Address of customer`.

Elements	Description
Add Data	Use the **Add Value** page to specify the data elements that are part of that actor. For an actor like Address, the attributes could be Address Line1, Address Line2, Address Line3, City, State, Zipcode, and Country. Define the data elements for each attribute of an actor by following these instructions: • **Name:** Specify a name for the attribute. For example, Address Line1. • **Description:** Specify a description for the attribute. For example, the address of the customer logging in. • **Required:** Use the toggle button to specify whether the element is required in the **Required** field. Some attributes are not required all the time because the actor can function without this data. For example, "Address Line2" in an address is not required since many addresses do not have this attribute. • **Data Type:** Specify the data type of the attribute. A data type is an attribute that specifies the type of data that the attribute can take: `Boolean`, `String`, `Numeric`, and `Date`. • **Encrypted:** Use the toggle button to specify whether the element should be encrypted. If **Encrypted** is set to`True`, data is encrypted so that it can be stored securely in the database to protect sensitive data. Encryption is used for string data fields only; other data fields are not required to be encrypted.

Activity Details

Details are unique for each monitored activity and therefore not reusable across different user activities. For example, the total dollar amount for a purchase activity would not be reused in multiple activities, so it should be custom data and not actor.

Example of custom data are as follows:

- Dollar Amount
- Coupon Code
- Item Number

After you create an actor, click **Next**, and then click **Add Details**.

Elements	Description
Name	Specify a name for the activity detail.
Description	Specify a description for the activity detail.
Required	Use the toggle button to specify whether the element is required in the **Required** field.

Elements	Description
Data Type	Specify the data type of the attribute. A data type is an attribute that specifies the type of data that the attribute can take: `Boolean`, `String`, `Numeric`, and `Date`.
Encrypted	Use the toggle button to specify whether the element should be encrypted. **Encryption is used for string data fields only**; other data fields are not required to be encrypted.

You must bear the following points in mind:

- You can enable a custom activity only when you have defined the mapping of all the actors or custom data that you have added in the custom activity.
- You cannot delete an enabled custom activity. You must first disable the custom activity, and then delete it.

2.3 Create New Actor

An actor is a data structure that you can reuse in multiple custom activities. For example, an address actor could be used as a shipping address, billing address, home address, and so on.

Elements	Description
Name	Specify a unique name of the actor. For example, for the Address actor, enter `Address` in the **Name** field.
Description	Specify the description of the actor. For example, you can enter `Address of customer`.

Elements	Description
Add Data	Use the **Add Value** page to specify the data elements that are part of that actor. For an actor like Address, the attributes could be Address Line1, Address Line2, Address Line3, City, State, Zipcode, and Country. Define the elements for each attribute of an actor by following these instructions: • **Name:** Specify a name for the attribute. For example, Address Line1. • **Description:** Specify a description for the attribute. For example, the address of the customer logging in. • **Required:** Use the toggle button to specify whether the element is required in the **Required** field. Some attributes are not required all the time because the actor can function without this data. For example, "Address Line2" in an address is not required since many addresses do not have this attribute. • **Data Type:** Specify the data type of the attribute. A data type is an attribute that specifies the type of data that the attribute can take: `Boolean`, `String`, `Numeric`, and `Date`. • **Encrypted:** Use the toggle button to specify whether the element should be encrypted. If **Encrypted** is set to`True`, data is encrypted so that it can be stored securely in the database to protect sensitive data. **Encryption is used for string data fields only**; other data fields are not required to be encrypted.

2.4 Create New Group

Groups are collection of similar items to simplify configuration workloads. You can use groups in the following items, such as Rule conditions, Actions, and Alerts.

To create a **Risky IPs** rule, you must add a condition to find out if the user IP used for login is in the list of risky IPs configured. These are grouped together as **Risky IPs** of type **IP** and the rule condition uses this group.

To create a group, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.
2. From the menu, click **Manage Groups**.
3. Click **Create New Group**.

New Group

Elements	Description
Group Name	Specify a name for the group.
Group Type	From the **Group Type** list, select the appropriate group.
Group Description	Specify a description for the group.
Value	Specify the value for the group based on the **Group Type** selected.

2.5 Create New Profile

Profiles record the behavior of the users, device and locations accessing the system by creating a digest of the access data. The digest or profile information is then stored in a historical data table and used for calculating the current risk using rules.

To create a profile, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.
2. From the menu, click **Manage Profiles**.
3. Click **Create New Profile**.

New Profile

Elements	Description
Profile Name	Specify a name for the profile.
Status	Specifies the status of the profile. From the **Status** list, select the appropriate status.
Description	Specify a description for the profile.
Activity Type	It is **Authentication** by default.
Member Types	From the **Member Types** list, select the required type of member. The member type is the actor for which data must be captured. For example, if you select `City` as the member type, the profile created collects city data. One or more member types can be selected for a profile.

Elements	Description
Add Property	Provide the following details about the property: • Property: From the **Property** list, select the required property. • Label: Specify a label for the property. • Description: Specify a description for the property. • Status: Specifies the status of the property. Use the toggle button to enable the property if you want OARM to collect data on the property to be used in the profile. • Compare Operator: Select a compare operator. The list of compare operators depends on the value of the property you have chosen. • Compare Value: Specify the value for comparison. **Note:** The details change based on the compare operator you select.

2.6 List User Activity Rules

Any operation performed by the user that requires monitoring can be termed as User Activity. For instance, logging in, user transaction's like retail banking, credit card based activity, and so on.

OARM provides an out-of-the-box user activity called **User Authentication** with a rich set of prepackaged rules that evaluates the user activity to detect commonly found threats and take remedial actions and raise alerts.

To view the User Activity rule list, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Adaptive Risk Management**.
2. From the **User Authentication** tile, click the **Rules** link.

User Activity

Elements	Description
Select User Activity	Provides a list of user activities, both User Authentication and custom.
Rule Outcome	Provides a list of rule types based on the outcome, such as `Block`, `Allow`, `Challenge`, and `All`.
Search Rule	Allows you to search a rule based on the specified text.
Add New Rule	Allows you to create a new rule.
Active	Specifies whether the rule is active or not.
Details	Displays information about a rule.
Edit	Allows you to edit a rule.
Delete	Allows you to delete a rule.

2.7 List User Sessions

The **User Sessions** page provides information about sessions and enables easy access to key information regarding a session, such as the session information, device information, location information from where the user logged in, user activities associated with the session, rules, actions, and alerts triggered for the session.

The **User Sessions** page displays an overview of the events that transpired during a specific session, which enables investigators and customer care personnel to investigate for fraud detection.

Example

You see a session with a Risky IP alert and a Block authentication status. In your experience, this combination is indicative of a fraud attempt. This may be a case of stolen authentication credentials that you want to investigate. You open the details screen for this session to review exactly what occurred in this session.

To view **User Sessions** page, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.
2. Click **Monitor User Sessions**.
3. From the menu, click the **Session** ID link of the session you are interested in.

The **User Sessions** page for that session is displayed.

The **User Sessions** page consolidates information needed for fraud detection.

It contains several panels that provide the information needed to investigate a session. They are as follows:

- **Session Information**: Contains all the general information related to that session, such as the user name, last updated on date and time, and internal session ID.
- **Device Information**: Contains information associated with the device that was used for the transaction, such as the device ID, device type, and the operating system.
- **Location Information**: Contains all the related information regarding the location of the user. It shows the IP address, country, and state from which the user logged in.
- **User Activities**: Contains information about the activity performed by the user. It shows you the action generated by the rule triggered for that activity and the time taken to execute the activity.
- The last panel contains information about the rules that were triggered, action performed, and alerts triggered for the investigators.

2.8 List Custom Activity

Lists all the custom activities.

To open the custom activity list, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.
2. From the menu, click **Custom Activities**.

Custom Activities

Elements	Description
Search	Specify the search string to locate a custom activity.
Create	Allows you to create a custom activity.
Active	Specifies whether the custom activity is active or not.
Edit	Allows you to edit a custom activity.
Delete	Allows you to delete a custom activity.

2.9 List OAAM Policies in the OAAM Policy Explorer

The OAAM Policy Explorer view is available to provide additional details about OAAM policies, rules, conditions, and trigger combinations. It lists all the OAAM policies that address basic registration and authentication flows in OAAM.

After transitioning from OAAM environment, you can view all your existing OAAM policies in the OAAM Policy Explorer.

The OAAM policy explorer page displays the **Policy Name**, **Policy Status**, **Checkpoint**, **Run Mode**, and **Update Time** information of the policies listed on the page.

OAAM Policies

To open OAAM policies list, perform the following steps:

1. Click the **Application Navigation** hamburger menu on the top left.
2. From the menu, click **OAAM Policy Explorer**.
   The **OAAM Policies** window appears. This page shows a list of all your OAAM policies that are transitioned.

2.10 List OAAM Policy Summary

The OAAM Policy Explorer displays information about OAAM policies, rules, conditions, trigger combinations, group linking, nested policies, and other items.

Summary

It provides an overview of the policy.

Rules

Details about the rule is shown in the Policy Explorer. It displays the status, scores, weight, conditions, and results of that rule.

Trigger Combinations

There is an option to view the trigger override combinations or to view all overrides. It shows the override information that was evaluated for this session including the nested policy information.

2.11 Edit Rule

Edit an existing rule.

To edit a rule, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Adaptive Risk Management**.
2. From the **User Authentication** tile, click the **Rules** link.
3. Click the **Edit** icon of the rule you want to modify.

Edit Rule

Elements	Description
Name	Modify the name of the rule.
Status	Modify the status of the rule.
Description	Modify the description of the rule.
Select Action	Modify the action as required by business if this rule is triggered.
Select Alert	Modify the alert as required by business if this rule is triggered.
Search Condition	Modify the condition associated with the rule.

2.12 Edit Group

You can update details about any group. This information includes group name and group description.

To edit a group, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.
2. From the menu, click **Manage Groups**.
3. Click the **Edit** icon of the group you want to modify.

Edit Group

Elements	Description
Group Name	Modify the name of the group.
Group Description	Modify the description of the group.
Value	Add or delete the values of the element associated with the group.

2.13 Edit Profile

You can update details of a profile.

To edit a profile, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.

2. From the menu, click **Manage Profiles**.
3. Click the **Edit** icon of the profile you want to modify.

Edit Profile

Elements	**Description**
Profile Name	Modify the name of the profile.
Status	Specifies the status of the profile. From the **Status** list, select the appropriate status.
Description	Modify the description of the profile.
Member Types	From the **Member Types** list, select the required type of member. The member type is the actor for which data must be captured. For example, if you select `City` as the member type, the profile created collects city data. One or more member types can be selected for a profile.
Add Property	Provide the following details about the property: • Property: From the **Property** list, select the required property. • Label: Specify a label for the property. • Description: Specify a description for the property. • Status: Specifies the status of the property. Use the toggle button to enable the property if you want OARM to collect data on the property to be used in the profile. • Compare Operator: Select a compare operator. The list of compare operators depends on the value of the property you have chosen. • Compare Value: Specify the value for comparison. **Note:** The details change based on the compare operator you select.

2.14 Edit Custom Activity

Edit an existing custom activity.

To edit a custom activity, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.
2. From the menu, click **Custom Activities**.
3. Click the **Edit** icon of the custom activity you want to modify.

Edit Describe Activity

Elements	Description
Enter a name for this Activity	Modify the name of the custom activity.
Description	Modify the description of the custom activity.

Edit an Actor

To modify an actor, click **Next**, and then do one of the following:

- Click **Select an Actor** to add an existing actor provided out-of-the-box to the custom activity. See Select an Actor for more information about how to select an actor.
- Click **Create New Actor**. See Create New Actor for more information about how to create an actor.
- Click the **Edit** icon for the actor you want to modify.

Edit Details

To modify the activity details for a custom activity, do one of the following:

- Click **Add Details**. See Activity Details for more information about how to add activity details.
- Click the **Edit** icon for the activity details you want to modify.

2.15 Manage Groups

You can perform a number of actions to manage a group.

To manage groups, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.
2. From the menu, click **Manage Groups**.
   The **Groups** page appears with a list of standard groups.

Groups

Elements	Description
Search	Allows you to search a group based on the provided search string.
All Group Types	From the **All Group Types** list, select a group based on which you want to search a group. Note: **All Group Types** is the default value used for search operation from the list on group types.
Create New Group	Allows you to create a group.

Elements	Description
More Actions (…)	Provides you import and export options as follows: • **Import Groups:** Allows you to import a group or multiple groups as a ZIP file that is exported from an OARM system. • **Export Groups:** Allows you to export a group or a set of groups as a ZIP file. Select the rows corresponding to the groups you want to export. • **Export All Groups:** Allows you to export all the listed groups as a ZIP file.
Edit	Allows you to edit an existing group.
Delete	Allows you to delete an existing group.

2.16 Manage Profiles

You can perform a number of actions to manage a profile, such as changing activity type, adding member types, adding a property, and so on.

To manage profiles, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left.
2. From the menu, click **Manage Profiles**.
   The **Profiles** page appears that allows you to manage a profile.

Profiles

Elements	Description
Create New Profile	Create a profile.
More Actions (…)	Provides you import and export options as follows: • **Import Profiles:** Allows you to import a profile or multiple profiles as a ZIP file that is exported from an OARM system. • **Export Profiles:** Allows you to export a profile or a set of profiles as a ZIP file. Select the rows corresponding to the profiles you want to export. • **Export All Profiles:** Allows you to export all the listed profiles as a ZIP file.
Search	Search a profile based on the provided search string.
Edit	Edit a profile.
Delete	Delete a profile.

2.17 Monitor User Sessions

The **User Sessions** page provides a consolidated view of all the user sessions, which further enables you to monitor a particular session for fraud analysis.

OARM provides the capability to gather detailed information about the session and to allow you to drill down further into the details involved in the session. For example, you need information to investigate logins so you perform a sessions search. Click Session ID to investigate the events that transpired during a specific session.

User Sessions

Elements	Description
Search box	In the **Search** field, specify the search text.
User Name	From the list, select the search criterion. By default, **User Name** is selected as a search criterion.
Include Successful Sessions	Use the toggle button to include sessions that are successful. By default, it is disabled, and provides only non-successful session information.
Time Range	Specify the time range for which you want to perform a search.

2.18 Configure Security Questions for Knowledge-Based Authentication

Knowledge-based authentication (KBA) is an authentication method which is used to challenge the user to prove identity based on the user’s answers substantiated by a real-time interactive question and answer process.

The **Security Questions** page provides information about managing tasks that impact challenge questions, validations and levels of logic algorithms used for answers, question categories, and levels of logic algorithms used for registration.

The **Security Questions** page manages the following key elements:

Elements	Description
Registration Logic	Manages the registration of challenge questions and answers. You can configure number of questions that a user must register, the number of questions that appear in each menu, and the number of categories per menu. The user is required to select one question from each menu and enter answers for them. Only one question from each question menu can be registered. To configure **Registration Logic**, you specify the settings for question set generation as follows: • **Questions User Will Register**: Refers to the number of questions that a user must register. The new user registration should display the same number of question menus as the number of questions that a user must register. • **Questions per Menu**: Refers to the number of questions that appear on each menu. **Note:** The total number of questions from all the menus (number of menus multiplied by the questions in each menu) cannot exceed the total number of questions available in the database. • **Categories per Menu**: Refers to the number of categories per menu. To learn more about the key concepts of registration logic, see Configuring Registration Logic.

Elements	Description
Answer Logic	Validates if the answer provided by the user matches with what was provided during registration. Answer Logic consists of advanced algorithms selected by the system to configure the level of tolerance of the erroneous answer. The algorithms are divided into three categories: Common Abbreviations, Keyboard Fat Fingering (accidentally pressing the nearest neighbor on the keyboard), and Phonetics. You can enable or disable the Answer Logic algorithms. You can also configure the strength of some algorithms, such as Keyboard Fat Fingering and Phonetics for evaluating answers given for challenge questions as follows: • **Off:** No Answer Logic is used. Answers must exactly match those provided at the time of registration. • **Low:** Low level of Answer Logic is used. Answers provided by the user must be a match or near-match to the answers that were provided at the time of registration. • **Medium:** More Answer Logic is used. You are given some freedom for the answers that are provided. For instance, St. is acceptable for Street. • **High:** Highest level of Answer Logic is used. The constraints are not strict for matching. To learn more about the key concepts of answer logic, see Configuring Answer Logic.
Top Categories	Lists the top five categories based on the number of questions linked with a category in descending order. The questions are grouped into several categories and the user can select questions from these categories. Click **View All Categories** link to see a list of standard categories that questions can be grouped into as follows: • Childhood • Sports • Your Birth • Parents, Grandparents, Siblings • Children • Your Employment • Significant Other • Pets • Automobile • Education • Miscellaneous

Elements	Description
Top Questions	Lists the five most used questions based on user and validation statistics. Click **View All Questions** link to view a list of supported questions. Click **View All Validations** link to view a list of supported validations.

2.19 List Categories

The questions are grouped into several categories and the user can select questions from these categories. The **Categories** page lists all the standard categories that questions can be grouped into.

To view the categories list, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Categories** panel, click the **View All Categories** link.
   The **Categories** page appears with a list of standard categories that questions can be grouped into.

Categories

Elements	Description
Search box	In the **Search** field, specify the text to search for the category you are interested in.
Create New Category	Create a category, if the standard categories do not meet your requirements.
Edit	Edit a category.
Delete	Delete a category.

2.20 Create New Category

If the standard categories that questions can be grouped under does not meet your requirement, then you can create categories that can hold pertinent questions you plan to create.

To create a category, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Categories** panel, click the **View All Categories** link.
3. Click **Create New Category**.
   The **New Category** page appears where you can enter details to create a category.

New Category

Elements	Description
Category Name	Specify a name for the category.
Category Description	Specify a description for the category.

2.21 Edit Category

Edit an existing category.

To edit a category, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Categories** panel, click the **View All Categories** link.
3. Click the **Edit** icon of the category you intend to modify.
   The **Edit Category** page appears where you can modify the details of a category.

Edit Category

Elements	Description
Category Name	Modify the name of the category.
Category Description	Modify the description of the category.
Status	Modify the status of the category: **Active**, **Disabled**, **Deleted**. To learn about the logic to handle disabled and deleted categories, see About Disabling Question and Category Logic and About Deleting Question and Category Logic.

2.22 List All Questions

The customer can configure a set of challenge questions that are used to authenticate users. The **Questions** page lists the standard challenge questions that are presented to the user at the time of registration.

To view the challenge questions list, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Questions** panel, click the **View All Questions** link.
   The **Questions** page appears with a list of standard challenge questions.

Questions

Elements	Description
Search box	In the **Search** field, specify the question text to search for in the category selected from the Categories drop-down menu.

Elements	Description
Create New Question	Create a question, if the standard questions do not meet your requirements.
More Actions (…)	Provides you import and export options as follows: • **Import Questions:** Allows you to import a question or multiple questions as a ZIP file that is exported from an OARM system. • **Export Questions:** Allows you to export a question or a set of questions as a ZIP file. Select the rows corresponding to the questions you want to export. • **Export All Questions:** Allows you to export all the listed questions as a ZIP file.
Edit	Edit a question.
Delete	Delete a question.

2.23 Create New Question

If the standard challenge questions do not meet your requirement, then you can create questions that are applicable to the users accessing your application.

To create a question, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Questions** panel, click the **View All Questions** link.
3. Click **Create New Question**.
   The **New Question** page appears where you can enter details to create a question.

New Question

Elements	Description
Question	Type the new question.
Category	From the **Category** list, select the category in which you want this question to appear.
Locale	Select a locale from the list of locales available.
Registration Validation	Select the validation type from the **Registration Validation** list to assign a validation. You can assign a validation to control the answers a user is allowed to register for this specific question.
Answer Logic Hints	From the **Answer Logic Hints** list, select the type of hint you want for the answer logic. A hint can be added to questions individually to evaluate given answers. This is especially important for date related questions.

Elements	Description
Status	Set the status of the question: **Active**, **Disabled**, **Deleted**. When the **New Question** page first appears, the default value for the question status is **Active**. To learn about the logic to handle disabled and deleted questions, see About Disabling Question and Category Logic and About Deleting Question and Category Logic.

2.24 Edit Question

Edit an existing question. Read-only question statistics are available in the **Question Statistics** panel.

To edit a question, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Questions** panel, click the **View All Questions** link.
3. Click the **Edit** icon of the category you intend to modify.
   The **Edit Question** page appears where you can modify the details of a question.

Edit Question

Elements	Description
Question	Modify the text of the question.
Category	From the **Category** list, modify the category in which you want this question to appear.
Locale	Modify the locale from the list of locales available.
Registration Validation	Modify the validation type from the **Registration Validation** list to assign a validation. You can assign a validation to control the answers a user is allowed to register for this specific question.
Answer Logic Hints	From the **Answer Logic Hints** list, select the type of hint you want for the answer logic. A hint can be added to questions individually to evaluate given answers. This is especially important for date related questions.
Status	Modify the status of the question: **Active**, **Disabled**, **Deleted**. To learn about the logic to handle disabled and deleted questions, see About Disabling Question and Category Logic and About Deleting Question and Category Logic.

2.25 List All Validations

Validations are used to validate the answers given by a user at the time of registration.

To view the validations list, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Questions** panel, click the **View All Validations** link.
   The **Validations** page appears with a list of standard validations.

Validations

Elements	Description
Search box	In the **Search** field, specify the text to search the validation that you want view.
Create New Validation	Create a validation, if the standard validations do not meet your requirements.
More Actions (…)	Provides you import and export options as follows: • **Import Validations:** Allows you to import a validation or multiple validations that is exported from an OARM system. • **Export Validations:** Allows you to export a validation or a set of validations as a ZIP file. Select the rows corresponding to the validations you want to export. • **Export All Validations:** Allows you to export all the listed validations as a ZIP file.
Edit	Edit a validation.
Delete	Delete a validation.

2.26 Create New Validation

You can create a validation when needed. Validations are defined to validate the answers given by a user at the time of registration.

To create a validation, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Questions** panel, click the **View All Validations** link.
3. Click **Create New Validation**.
   The **Validations** page appears where you can enter details to create a validation.

> **Note:**
>
> The fields displayed on the **Validations** page depends on the validation type selected from the **Select Validation Type** list.

Validations

Elements	Description
Select Validation Type	From the **Select Validation Type** list, select the validation type you want to add.

Elements	Description
Name	Specify the name for this instance of the validation.
Validation Parameter	Specify the validation parameter that corresponds to your validation type. For example, validation parameter **Enter Maximum Length** can be 30 for an instance of Maximum Length validation type. This validation instance restricts the user from entering an answer longer than 30 characters in length. Following validation parameters are supported for respective validation type: **Repeated Character, Inappropriate Language, Minimum Length, Maximum Length, Repeated Answers, Date, Regular Expression, Character**. To learn more about the validation parameters, see the following table.
Error Message	Specify an error message for this instance of validation.

Validation Parameters

Validation Type	Description	Example
Repeated Character	Allowed number of repeated characters in the answer. If the answer entered by the user contains repeated characters more than the configured value, the validation fails and the user gets a configured error message.	3
Inappropriate Language	Inappropriate language for answer.	Sloppy,Wrong,Yucky The list of words should not contain blank spaces.
Minimum Length	Minimum length (number) for the answer. If the length of the answer entered by the user is less than the configured value, the validation fails and a configured error message is displayed.	4
Maximum Length	Maximum allowed length (number) for the answer. If length of the answer entered by the user is above the configured value, the validation fails and a configured error message is displayed.	4

Validation Type	Description	Example
Repeated Answers	Allowed number of repeated answers. For example parameter value can be '1' for unique answer validation. If the answer entered by the user is repeated more than configured number of times, the validation fails and the user gets a configured error message.	1
Date	Date/Time pattern string for the answer. For example, the pattern can be "MMddyy" for Month Day Year validation. If the date/time answer entered by the user is not as per the configured pattern, the validation fails and a configured error message is displayed.	MMDDYY
Regular Expression	Real expression pattern string for the answer. For example, pattern can be "[A-Za-z0-9]+" for Alpha-numeric validation. If the answer entered by the user is not as per the configured regular expression pattern; then, the validation fails and a configured error message is displayed.	[0-9]+
Character	Characters that are allowed.	*

2.27 Edit Validation

Edit an existing validation.

To edit a validation, perform the following steps:

1. Click the **Application Navigation** hamburger menu on top-left and click **Configure Security Questions**.
2. From the **Top Questions** panel, click the **View All Validations** link.
3. Click the **Edit** icon of the validation you want to modify.
   The **Edit Validation** page appears where you can modify the details of a validation.

Edit Validation

Elements	Description
Validation Parameter	Edit the validation parameter that corresponds to your validation type. You can edit the following validation parameters supported for respective validation type: **Repeated Character, Inappropriate Language, Minimum Length, Maximum Length, Repeated Answers, Date, Regular Expression, Character**.
Error Message	Edit the error message for this instance of validation.