Oracle® Adaptive Access Manager

Administrator's Guide

Release 10*g* (10.1.4.5)

E12055-03

May 2009

ORACLE®

Oracle Adaptive Access Manager Administrator's Guide, Release 10*g* (10.1.4.5)

E12055-03

Primary Author: Priscilla Lee

Contributors: Mandar Bhatkhande, Sree Chitturi, Josh Davis, Bosco Durai, Luke Harris, Prakash Hegde, Daniel Joyce, Mark Karlstrand, Derick Leo, Karl Miller, Valarie Moore, Srinivas Nagandla, Madhan Neethiraj, Paresh Raote, Jim Redfield, Uday Sambhara, Kamal Singh, Nandini Subramani, Vidhya Subramanian, Sachin Vanungare, and Saphia Yunaeva

Contents

3 Rules and Models

4 Rule Templates and Conditions

5 Configurable Actions

12 Reporting

Part V Using Adaptive Risk Manager Offline

13 Using Adaptive Risk Manager Offline

14 Troubleshooting

Part VII Appendices

A Conditions Reference

Preface

The *Oracle Adaptive Access Manager Administrator's Guide* provides information on managing groups, models, rules, rules templates and conditions; managing configurable actions; creating runtimes, creating transaction definitions; managing Auto-learning and patterns, managing Knowledge-based Authentication (KBA) challenge questions; creating and managing cases; monitoring alerts using the dashboard; running queries and creating reports; loading and running data for evaluation offline, and troubleshooting.

This Preface covers the following topics:

Audience

The audience for the Oracle Adaptive Access Manager Administrator's Guide includes:

- Fraud Analysts—The fraud analyst identifies potential and existing fraudulent activities that could occur against the organization's online applications and defines the parameters for each potential fraudulent activity.
- Rule Designers—The rules designer groups fraud scenarios into logical models and maps potential fraudulent activity into an implementation design to be used by the rules engineer.
- Rules Engineers—The rules engineer configures the fraud management tool to protect against the potential fraudulent activity, monitors the fraud tool to identify fraudulent attempts and opportunities for optimization, and reports fraudulent attempts.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be

accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For more information, see the following documents in the Oracle Adaptive Access Manager 10.1.4.5 documentation set:

- *Oracle Adaptive Access Manager Release Notes*
- *Oracle Adaptive Access Manager Reference Guide*
- *Oracle Adaptive Access Manager Developer's Guide*
- *Oracle Adaptive Access Manager Concepts*
- *Oracle Adaptive Access Manager Installation and Configuration Guide*

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.

What's New

This section describes new features of Oracle Adaptive Access Manager 10g (10.1.4.5).

New Features for Release 10.1.4.5

These are the features introduced in the current release:

- Auto-learning

  Auto-learning is a profiling process in which Adaptive Risk Manager identifies behavior patterns (buckets) based on the parameters the administrator specifies. Adaptive Risk Manager then automatically records/maintains the bucket memberships of the users/devices/locations (entities in general) over time so that the data that is gathered can be used as a way to evaluate risk. For more information, see Chapter 8, "Auto-learning and Patterns".

- Rule Template Editor

  The rule template editor allows the user to create and edit rule templates without having to go to the XML and write them. For more information, see Chapter 4, "Rule Templates and Conditions".

- Configurable Actions

  Configurable Actions allow a user to create new supplementary actions that occur after the running of rules. For more information, see Chapter 5, "Configurable Actions".

- Transaction Definitions

  Oracle Adaptive Access Manager provides a framework to support any kind of transaction by mapping client-specific data into the generic data model that supports the framework. For more information, see Chapter 7, "Transaction Definitions".

- Device registration

  Device registration is a feature that allows a user to flag the device (computer, mobile, PDA, and others) he is using as a safe device. The customer can then configure the rules to challenge a user that is not coming from one of his registered devices. Device registration is available as a standard feature in Oracle Adaptive Access Manager. The feature can be turned on, although it is turned off by default in the product. For more information, see Chapter 10, "Cases".

- Enumeration Editor

An enumeration contains named constants to represent different possible values. In Oracle Adaptive Access Manager, these enumerations (enums) are defined so they are easily configurable by the administrators; no code change is necessary.

Using the enumeration editor, existing enumerations and their elements and properties can be edited in Adaptive Risk Manager. New enumerations can also be created to customize Adaptive Risk Manager.

For more information, see Chapter 6, "Creating Runtimes".

- Investigation tools

  Investigation management offers tools needed by fraud investigators (agents) to conduct investigation process. A new case type, agent cases enable fraud investigation agents to obtain information and track the progress of the investigation (case lifecycle). Linked sessions and related sessions and cases provide investigators a way to quickly narrow in on the important data they need to resolve a case. For more information, see Chapter 10, "Cases".

- Customizable reporting using BI Publisher

  Starting with the 10.1.4.5 release, export and scheduling of reports are available via Oracle BI Publisher. Oracle BI Publisher provides a much richer functionality – support for more export file formats and schedule options. This guide contains details of Oracle Adaptive Access Manager reports in Oracle BI Publisher.

  Reports are editable through the BI Publisher. Column labels and contents can be editable. Also, aggregates and graphing can be added to reports. For more information, see Chapter 12, "Reporting"

- Globalization Support

  Oracle Adaptive Access Manager 10.1.4.5 has been translated into 26 languages for Adaptive Strong Authenticator and 9 for Adaptive Risk Manager. These translations are bundled along with the English version of the product. For additional information, see "Globalization Support" in the *Oracle Adaptive Access Manager Installation and Configuration Guide*.

- Conditions

  Rule conditions are the building blocks for constructing rule templates. Oracle Adaptive Access Manager includes a library of preconfigured conditions. For more information, see Chapter 4, "Rule Templates and Conditions"

- Dashboard

  Adaptive Risk Manager includes a dashboard that provides performance and summary statistics and reports on locations, scoring, devices, security, and performance. For more information, see Chapter 11, "Using the Dashboard"

Part I

Administration

Part I contains the following chapters:

1
Introduction

Oracle Adaptive Access Manager provides fraud management in multiple ways. Oracle Adaptive Access Manager and its components effectively reduce fraudulent activities by detecting and providing remedial actions in real time.

Oracle Adaptive Access Manager is composed of two primary components: Adaptive Strong Authenticator (ASA) which provides front-end protection against online identify theft and Adaptive Risk Manager (ARM) which provides real-time, fraud detection.

- **Adaptive Strong Authenticator**: When a user signs in to a Web site, Adaptive Strong Authenticator can present zero, one, or more challenges to the user. The simplest challenge is a password while more complex challenges are questions selected from a list of pre-answered questions. The answer forms may use a physical keyboard or a virtual keyboard or keypad and mouse to prevent malicious keyboard loggers from intercepting keystrokes.
- **Adaptive Risk Manager**: When User A signs in to Web site B, Adaptive Risk Manager evaluates several criteria to determine how likely the user is who he or she claims to be. A series of scores are calculated based on factors such as whether this is the user's "normal" terminal, the "normal" IP address, the "normal" time-of-day. Each of the scores is then multiplied by a configurable weight for a total risk assessment. As the level of confidence goes down, a stronger challenge is presented to the user beyond the normal password. Certain sensitive transactions after login might also trigger another challenge to reconfirm that the user has not exited the session. This risk assessment can be performed in real time or offline. The application that is being protected can be either aware of the Adaptive Risk Manager through APIs or not. Certain Web servers can be automatically redirected to use the Adaptive Risk Manager using the Universal Installation Option with no modification of the application code.

The audience for the *Oracle Adaptive Access Manager Administrator's Guide* includes:

- Fraud Analysts—The fraud analyst identifies potential and existing fraudulent activities that could occur against the organization's online applications and defines the parameters for each potential fraudulent activity.
- Rule Designers—The rules designer groups fraud scenarios into logical models and maps potential fraudulent activity into an implementation design to be used by the rules engineer.
- Rules Engineers—The rules engineer configures the fraud management tool to protect against the potential fraudulent activity, monitors the fraud tool to identify fraudulent attempts and opportunities for optimization, and reports fraudulent attempts.

1.1 Concepts

To get started using Oracle Adaptive Access Manager you need to import or create models and rule templates. You configure new models by creating the component rules, defining manual overrides to control the behavior of the rules, and connecting the models to the target groups. Here's an overview of the component parts of models and rules:

- **Auto-learning**—Auto learning is a feature that analyzes the behavior of user data coming into the system and profiles (creates digest) of the user's data. This data is then stored in a historical data table and used for calculating the risk based on Rules. The best advantage of Auto-learning is that the system learns the changes in user's behavior and slowly adapts to it when calculating risk.
- **Buckets**—Auto-learning patterns are used to dynamically create and populate profiling buckets to track behavior and transactions.
- **Entity**—A referencible data structure that can be used in transaction definitions or directly in patterns.
- **Groups**—Groups allow you to view and administister a collection of like items as a single group. You should assign each group a unique name. The types of groups you can create include User ID, Login ID, Location, Device, Action, and Alert.
- **Model**—A model is a set of rules that run at a single time. A model contains configured rule instances (copies of rules) that when linked to a group, are used to evaluate group members. The rules are added to the model, configured, and linked to groups by the administrator. A new rule instance can be added to an existing model at any time. In a model, you can control the timing and combinations of rule firing with manual overrides.
- **Patterns**—Profiling is configured by the creation of patterns that define the type and amount of data collection to be done.
- **Policy**—A policy is a collection of models of the same type. The policy types are Security and Business.
- **Policy Sets**—A policy set is the collection of all the currently configured policies used to evaluate traffic to identify possible risks. As a fail-safe, an action override or a score override can be created for a policy set so that the override is automatically invoked to override a particular action triggered by a rule when a specific set of circumstance occurs.
- **Rule Conditions**—Rule conditions are the building blocks for constructing rule templates and make the rule-related functions in Oracle Adaptive Access Manager available to the client.
- **Rules**—A rule is also known as a rule instance. A rule triggers an outcome. A rule identifies and reacts to certain information. Rules can be used for security or business purposes. Rules can be added to Models, and Models can be applied to a group of users or all users.
- **Rule Template**—The rule template forms the basis for creating a rule instance. Adding condition instances to rule templates allow you to create the template you need for your use cases. Rule templates must have at least one condition.
- **Runtime**—A Runtime is a specified point in a session when rules in a model will run. For example, at pre-authentication, post-authentication, and in-session.
- **Scores & Weights**—Score refers to the numeric scoring used to evaluate the risk level associated with a specific situation. Weight refers to the multiplier used to

influence the total score at various evaluation levels. Weight is only applied to a score when a given Policy Type is using a "weighted" scoring engine.

- **Transaction Definition**—Application data is mapped using the transaction definition before transaction monitoring and profiling can begin. Each type of transaction Oracle Adaptive Access Manager deals with should have a separate transaction definition.

1.2 Fraud Management Steps

The following steps are best practices for the discovery/planning process. They are not actual steps to be taken in the application's user interface.

1. Identify fraud scenarios and derivative scenarios.
2. Define parameters for each derivative fraud scenario.
3. Group the relevant fraud scenarios, or derivatives, or both.
4. Map parameter and group details into implementation design.
5. Use mappings to configure Oracle Adaptive Access Manager.

1.2.1 Identify Fraud Scenarios and Derivatives

A fraud scenario is a potential or actual deceptive situation involving malicious activity directed at a company's online application. Fraud scenario derivatives are the different sub-scenarios that support the existence of the parent fraud scenario. These fraud scenario and derivatives must be mapped into rules to protect against fraudulent behavior.

To identify a fraud scenario derivative, start by doing the following:

- Identify *gated security* checkpoints and Runtimes
- Define transaction entities and attributes using data models for each of those Runtimes

1.2.2 Define Parameters for Each Derivative Fraud Scenario

The parameters are the details in the derivatives. These details specifically are the datapoints that are used to compare against a threshold to determine an outcome.

A threshold is the quantitative point at which an action is triggered. For example, a threshold might be ten authentication attempts within 24 hours. An outcome is the response initiated when a threshold is satisfied and a rule is triggered. For example, an outcome might be twofold: an action event activated and an alert message activated.

Datapoints are classified in one of two categories:

- Runtime Datapoints—Runtime datapoints are the entities and attributes that exist in a current transaction.
- Historical Datapoints—Historical datapoints are the entities and attributes that exist in past transactions.

1.2.3 Group the Relevant Fraud Scenarios, or Derivatives, or Both

You first group the fraud scenarios into models and then you assign the models to an Oracle Adaptive Access Manager policy.

1.2.3.1 Grouping Derivatives into Models

Fraud scenario derivatives are grouped into models based on the following considerations:

1. Identify the derivatives that logically fit together:
   - Manageability: derivatives have like policies (for example, application specific).
   - Similarity: derivatives are trying to detect or prevent like fraud instances (for example, Brute Force).
   - Dependencies: derivatives have relationships (for example, if this and this is true do this).
   - Risk: derivatives are evaluated based on previous risk scores.
2. Validate each model based on a single Runtime.
3. Evaluate models to eliminate redundancies.

1.2.3.2 Assigning Models to Policies

After you define the models and assign the fraud scenario derivatives to the models, the models need to be assigned to an Oracle Adaptive Access Manager policy. These Policies include:

- Security Policy—A Security Policy is based on cross-industry best practices.
- Business Policy—A Business Policy is based upon parameters established for mitigation of transaction risk

1.2.4 Map Parameters and Group Details into an Implementation Design

The Implementation Design includes all the fields necessary to configure Oracle Adaptive Access Manager. This requires a mapping of the existing data to the Oracle Adaptive Access Manager fields.

Existing data include:

- Fraud Scenario Derivatives
- Parameters, Thresholds & Outcomes
- Policies & Models

Oracle Adaptive Access Manager fields include:

- Rule Template Name
- Model Name
- Alert Group
- Action Group
- Affected Group(s)
- Score

1.2.5 Use Mappings to Configure Oracle Adaptive Access Manager

Finally the Implementation Design is used to configure Oracle Adaptive Access Manager.

1.3 Knowledge-Based Authentication

Oracle Adaptive Access Manager provides out of the box secondary authentication in the form of knowledge based authentication questions. The KBA infrastructure handles registration, challenge and customer service of questions. KBA challenges can be presented online or over the phone by a customer service representative.

You can extend or customize the base models to support additional business and security requirements. Additionally, models can be easily configured for exceptions.

1.4 Reporting

Limited reporting is available through the Adaptive Risk manager application. In addition, a limited license of Oracle Business Intelligence Publisher is included for customizable reporting capabilities.

2

Managing Groups

Grouping enables you to view and administer a collection of like items as a single group. Adaptive Risk Manager Online enables you to create groups for more efficient administration.

This chapter provides information on creating, editing, and importing and exporting groups.

2.1 Organizing Users, Locations, and Devices into Groups

This section describes how to add items to groups individually. Auto-population and bulk uploads directly in the database are also available as part of the custom installation and integration process.

2.1.1 Creating User, Location, and Device Groups

This section describes how to create and edit user ID, location, and device groups.

2.1.1.1 Create a new group of user IDs

To create a new group of user IDs

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Group page appears.

2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and select User ID.
4. User groups do not support caching policy so it should be set to None.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.

7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.

9. In the User Id box, type the user Id of a user member you want to add to the group, and then click Add.

   The User ID appears in the list of Member Users.

2.1.1.2 Create a group of cities

To create a group of cities

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Groups page appears.
2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and choose Cities.
4. Click in the Caching Policy box and select the caching policy you want.

   Refer to "Caching Policy Options" for details about caching policy options.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.
9. Click in the Country box and choose the country you want.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.
10. Click in the State box and choose the state you want.
11. In the list of Available Cities, click the city you want to add, and then click Add.

2.1.1.3 Create a group of states

To create a group of states

1. On the Admin menu point to Groups, and then click Create Group.
2. In the Group Name box, type a unique name for the group.

   The Create Group page appears.
3. Click in the Group Type box and choose States.
4. Click in the Caching Policy box and select the caching policy you want.

   Refer to "Caching Policy Options" for details about caching policy options.

   Generally the full cache setting gives the best performance.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.
9. Click in the Country box and choose the country you want.
10. In the list of Available States, click the state you want to add, and then click Add.

2.1.1.4 Create a group of countries

To create a group of countries

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Group page appears.
2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and choose Countries.
4. Click in the Caching Policy box and select the caching policy you want.

   Refer to "Caching Policy Options" for details about caching policy options.

   Generally the full cache setting gives the best performance.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.
9. In the list of Available Countries, click the country you want to add, and then click Add.

2.1.1.5 Create a group of IP

To create a group of IP

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Group page appears.
2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and choose IPs.
4. Click in the Caching Policy box and select the caching policy you want.

   Refer to "Caching Policy Options" for details about caching policy options.

   Generally the full cache setting gives the best performance.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.
9. Type the IP address you want to include in the group, and then click Add.

2.1.1.6 Create a group of IP ranges

To create a group of IP ranges

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Group page appears.
2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and choose IP Ranges.
4. Click in the Caching Policy box and select the caching policy you want.

   Refer to "Caching Policy Options" for details about caching policy options.

   Generally the full cache setting gives the best performance.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.
9. Select from the list of Available IP Ranges, click the IP range you want to add to the group and click Add.

   If none exist you can create new IP ranges from the Admin menu.

2.1.1.7 Create a group of devices

To create a group of devices

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Group page appears.
2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and choose Devices.
4. Click in the Caching Policy box and select the caching policy you want.

   Refer to "Caching Policy Options" for details about caching policy options.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.
9. To search for devices, enter search criteria to limit returns and click Submit Query.
10. Select any number of devices from the list of available devices and click Add.
11. To add a specific device to the group without running a query, click in the Device ID box at the bottom of the page, type the device ID and click Add.

2.1.2 Creating a Group of Alerts or Actions

An actions group is a set of responses that are triggered by a rule.

An alert group contains graded messages that can be triggered by a rule.

Action groups and alert groups are used as results within rules so that when a rule is triggered all of the actions or alerts within the groups are activated.

This section describes how to place a selection of actions into a group and how to configure/add alerts to a group.

2.1.2.1 Create an action group

To create an action group

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Group page appears.
2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and choose Actions.
4. Action groups are always cached so Caching Policy should be set to Full Cache.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.
9. In the list of Available Actions, click the action you want to add to the group, and then click Add.

2.1.2.2 Create an alert group

To create an alert group

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Group page appears.
2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and select Alerts.
4. Alert groups are always cached so Caching Policy should be set to Full Cache.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The name of the group you are editing is pre-selected in the list of Groups.
9. Click in the Alert Level box and select the alert level you want.

10. Click in the Alert Type box and select the alert type you want.
11. Type an alert message. In most cases this message should correspond to the rule that will be configured to activate it.
12. Click Add.

2.1.3 Creating Groups of Networks, Service Providers, and Systems

In addition to user, location, device, alert, and action groups, Adaptive Risk Manager Online enables you to create these group types:

- ISP
- ASN
- Top Level Domains
- Second Level Domains
- Ip Carriers
- Routing Type
- Connection Type
- Connection Speed
- Generic Strings
- Generic Integers
- Generic Longs

To create a network, service provider, or system group

1. On the Admin menu point to Groups, and then click Create Group.

   The Create Group page appears.
2. In the Group Name box, type a unique name for the group.
3. Click in the Group Type box and select the type you want.
4. Click in the Caching Policy box and select the caching policy you want.

   Refer to "Caching Policy Options" for details about caching policy options.
5. Type any description and notes you want.
6. Click Create.

   The Group Details page appears.
7. To change the group's name, type, or notes, see "Viewing Details about a Group".
8. Click Edit Group.

   The Edit Groups page appears. The group you are editing is pre-selected.
9. In the String Value field, enter the value you want.
10. Click Add.

2.1.4 Editing a Group

You can edit a group whenever you want.

To edit a group

1. On the Admin menu point to Groups, and then click Edit Groups.

   The Edit Groups page appears.

2. To filter the list of groups, click in the Group Type box and select the type you want.

3. In the list of Groups, select the group you want to edit.

   The Edit Group page appears and displays the options appropriate for the type of group you selected.

4. Add or delete members of the group as necessary.

   For additional information, see "Creating a Group of Alerts or Actions".

2.1.5 Updating a Group Directly

You can update a group directly in the XML file. For example, you can perform a bulk update to a blacklisted IP group based on a monthly list of high risk IPs gained from a 3rd party service.

To update a group directly

1. Export the group you want to update.
2. Open the XML and make the edits you want.
3. Import the group to either overwrite or append to the previous version.

2.1.6 Exporting and Importing a Group

You can use the Export and Import Groups commands to export and import a group as an XML file.

2.1.6.1 Export a group

To export a group

1. On the Admin menu, point to Groups and click then click Export Groups.

   The Export Groups page appears.

2. Enter search criteria and click Run Query to locate the group.
3. Click the check box next to each group you want to export.
4. Click Export in the lower right corner of the page.
5. Click OK to the confirmation.

   The Open dialog box appears.

6. Click Save To Disk and then click OK.

   The file is exported.

2.1.6.2 Import a group

To import a group

1. On the Admin menu, point to Groups and click then click Import Groups.

   The Import Groups page appears.

2. Click Browse and locate the group file you want to import.
3. Click Import.

The group is imported.

2.1.7 Viewing a List of Groups

On the List Groups page, you can view a list of all groups, a list of groups of a certain type, or you can view just one group. The List Groups page provides access to the Group Details page and the Edit Group page for any group.

To view a list of all groups

1. On the Admin menu, point to Groups, and then click List Groups.

   The List Groups page appears.

2. To display only the type of group you want to edit, select the type you want from the Group Type list and click Submit Query.
3. To find a specific group, in the Group Name box enter the name of the group and click Submit Query.
4. To edit a group in the list, click the wrench icon to the left of the group you want to edit.
5. To view the Details for a group, click the Group Name.

   See "Viewing Details about a Group".

6. To delete a group, select the check box to the left of the group name and then click Delete.

   If the group is currently linked to a rule you will not be allowed to delete it.

2.1.8 Viewing Details about a Group

The Group Details page enables you to view or change details about a group.

To modify details about a group

1. On the Admin menu point to Groups, and then click List Groups.

   The List Groups page appears.

2. Select the search criteria you want and click Submit Query.
3. Click a group name to view the details page for that group.

   The Group Details page appears.

4. To change the group name, click in the Group Name box and type a new name and then click Save.

2.1.9 Caching Policy Options

Groups offer two caching policy options: Full Cache or None.

The "Full Cache" option caches group contents in server memory for the lifetime of the server. Static lookup groups, read-only groups, are good candidates for the "Full Cache" option. Administrators need to be careful using this option as it uses server memory. A long list of elements can have an adverse affect since groups are re-cached if there are changes to the list.

The "None" Caching Policy option does not use cache and consults the database every time. Devices and USER ID groups are defaulted to "None" because in most cases, they are dynamic and manipulated while the server is running. If you have Devices and

USER ID type groups that stay static for the lifetime of the server, you can use the "Full Cache" option instead of "None."

3

Rules and Models

A model is a collection of configured rule instances linked to User ID groups whose members are evaluated. Adaptive Risk Manager enables you to create models that can be applied to more than one User ID group.

This chapter provides information about creating and editing models, importing and exporting model, and adding and customizing rules.

3.1 Creating and Editing Models

Oracle Adaptive Access Manager is shipped with groups, models and rules preconfigured. These models are set up using best practices for the client's specific industry and needs.

3.1.1 Creating Models

Model Runtime refers to the point during the session the rules in a model should be evaluated. By default there are eleven model Runtimes in Adaptive Risk Manager Online:

- Device Identification
- Pre-Authentication
- Post-Authentication
- In-Session
- AuthentiPad
- Preferences
- Challenge Question
- CSR KBA Challenge
- Forgot Password
- Invalid Login
- Wrong Password

Note: "In-Session models often require custom integration and therefore configuration is not covered as part of this guide.

Note: "In-Session models are not supported in some Universal Installation Option version 1.0 installations.

1. On the Admin menu point to Models, and then click Create Models.

   The Policy Type menu appears.

2. In the Policy Type list, click the type of model you want.

   The Runtime menu appears.

3. In the Runtime list, click the Runtime you want.

   The Model Name menu appears.

4. In the Model Name list, click Create New Model.

   The Create New Model page appears.

5. In the Model Name box, enter a name for the model.

6. Click in the Status box and select the status you want.

7. Click the Run Mode box and select the option you want.

   Linking a model to a group enables the model to execute/run for the set of users within the linked group.

   Run Mode provides "All Users" and "Linked Users" as options. The default is "Linked Users" in which the model will only act on that user group. The "All Users" option links a model to all users.

   Note: If there are no group linkings, but "Linked Users" have been selected, then this model will not be executed at all.

8. Click in the Scoring Engine box and select the scoring you want.

9. In the Weight field, enter the weight you want.

10. In the Description box, enter a description of the model.

11. Click Save.

    The Model Details page for the new model appears.

3.1.2 Editing a Model

You can edit a model's general information and add or delete rules as needed

1. On the Admin menu point to Models and then click List Models.

   The List Models page appears.

2. Enter the search criteria you want and click Run Query.

3. On the List Models page, click the name of the model you want to edit.

   The Model Details page appears.

4. To edit the model's general information, make the changes you want at the top of the page and then click Save.

   The Model Details page provides tabs to the Rules page, Manual Overrides page, and Groups Linking page.

3.1.3 Exporting and Importing a Model

You can use the Export and Import Models commands to export and import a model as an XML file.

3.1.3.1 Export a Model

To export a model:

1. On the Admin menu, point to Models then click Export Models.

   The Export Models page appears.

2. Enter search criteria and click Run Query to locate the model.
3. Click the check box next to each model you want to export.
4. Click Export in the lower right corner of the page.
5. Click OK to the confirmation.

   The Open dialog box appears.

6. Click Save To Disk and then click OK.

   The model is exported.

3.1.3.2 Import a Model

To import a model:

1. On the Admin menu, point to Models and click Import Models.

   The Import Models page appears.

2. Click Browse and locate the model file you want to import.
3. Click Import.

   The model and all of the groups attached to the model are imported.

3.1.4 Document Models

The Document Models page enables you to view each model's composition. You can also print a document containing these settings.

1. On the Admin menu, point to Models and click Document Models.

   The Document Models page appears.

2. To find a specific model, enter the name of the model in the Model Name field and click Run Query.
3. To find models with a specific Runtime, in the Runtime list, click the Runtime you want and click Run Query.
4. To find models with a specific policy type, in the Policy Type list, click the policy type you want and click Run Query.
5. To find models with a specific status, in the Model Status list, click the status you want and click Run Query.
6. To generate an HTML document of the rule settings in a model, select the model you want and click Generate Document.

3.1.5 Policy Sets

Only one Policy Set is active and present in the system at a given time. The Policy Sets page displays the policy set used to evaluate traffic to identify possible risks. This page provides access to the Policy details page where you can specify the scoring engine and the weighting you want to use for evaluating risk.

Oracle Adaptive Access Manager uses the scoring engine to calculate the numeric score applied when calculating risk level. It then applies the weight—or multiplier value—to the score to determine its influence on the total score.

3.1.5.1 View a list of policy sets

To view a list of policy sets:

1. On the Admin menu, point to Policy Sets and then click List Policy Sets.

   The Policy Sets page appears and displays the Policy Set ID and Scoring Engine for each policy set in the system.

2. To view details about a policy set, click the Policy Set ID you want.

3.1.5.2 View and edit the policy set details

On the policy set details page you can specify the scoring engine used to calculate the score for the policy set that you want to use.

To view and edit the policy set details:

1. On the Admin menu, point to Policy Sets and then click List Policy Sets.

   The Policy Sets page appears.

2. Click the Policy Set ID you want.

   The Policy Set Details page appears and displays the scoring engine and the policy weights for the Policy Types included in the Policy Set. Each policy type contains all the corresponding models.

3. To change the policy weight, in the Scoring Engine list, select the scoring engine you want and click Save.

3.1.5.3 View and edit the policy details for a specific policy type

To view and edit the policy details for a specific policy type:

1. On the Policy Set Details page, click the Policy Type you want.

   The Policy Details page appears.

2. To change the Scoring Engine, in the Scoring Engine, select the scoring engine you want.

3. To change the weight percentage, enter the percentage you want in the Weight field.

4. Click Save.

3.1.6 Action and Score Overrides

You can create an Action Override or a Score Override as a failsafe which is automatically invoked to override the action triggered by a rule when a specific set of circumstance occurs.

3.1.6.1 Create an action override

You can create an Action Override to specify the action to replace the action triggered by individual rule. For example, an action override, which is based on "time" and "action," can be used to limit the number of blocks or to control the number of registrations with a specified timeframe.

To create an action override:

> **Note:** If a user/device/IP is already presented with the action in the given duration, it continues to get the same action and override will not apply.

1. On the Admin menu, point to Policy Sets and then click List Policy Sets.

   The Policy Sets page appears.

2. Click the Policy Set ID you want.

   The Policy Set Details page appears.

3. Click in the Action Override tab.

   A list of existing action override appears.

4. Click Add New.

   The Add New Block panel appears.

5. Click in the Runtime box and select the Runtime you want this override to apply to.

6. Click in the From Action box and select the action that you want to convert.

   For example, you might select Block so that you can convert the block to a challenge question.

7. Click the To Action and select the action to which you want to convert the action.

   For example, you might select Challenge to convert a block to a challenge.

8. Click in the Alert Group box and select the alert group you want generated when this event occurs.

   Alerts are indicators (messages) to personnel (CSR, Investigators, and so on). An alert group contains graded messages that can be triggered by a rule.

   Alert groups are used as results within rules so that when a rule is triggered all of the alerts within the groups are activated.

9. Click in the Sliding Window and enter the number of minutes within which you want the To Action to be triggered.

   For example, you might enter the number "30" so that if within 30 minutes there are more than 100 block, the system will stop blocking people and start challenging those people who would have been blocked.

10. In the Count field, enter the number of events generated by the From Action.

    For example, you might enter "100" to indicate more than ten blocks.

11. Click Add.

3.1.6.2 Create an score override

You can create a Score Override to specify an action group and/or alert group you want to be triggered when a score falls within a specific range. For example, if you have set a minimum score of 500, you can specify an action or alert group that you want to be triggered when the score reaches 501.

An actions group is a set of responses that are triggered by a rule. Action groups are used as results within rules so that when a rule is triggered all of the actions within the groups are activated.

Alerts are indicators to personnel (CSR, Investigators, and so on). An alert group contains graded messages that can be triggered by a rule. Alert groups are used as results within rules so that when a rule is triggered all of the alerts within the groups are activated.

To create an score override:

1. On the Admin menu, point to Policy Sets and then click List Policy Sets.

   The Policy Sets page appears.

2. Click the Policy Set ID you want.

   The Policy Set Details page appears.

3. Click the Score Override tab.

   A list of existing score override appears.

4. Click Add New.

   The Add New Score Action panel appears.

5. Click in the Runtime box and select the Runtime you want this override to apply to.

6. Click in the Action Group ID box and select the action that you want triggered in an override.

7. Click in the Alert Group ID box and select the alert to which you want triggered in an override.

8. Click in the Minimum Score field and enter the minimum score allowed before the score override is triggered.

9. Click in the Maximum Score field and enter the maximum score allowed before the score override is triggered.

10. Click Add.

3.1.7 Adding a New Rule to a Model

A rule defines an operation applied by the system to a specified user, device, or location group when a situation is detected that may indicate fraud.

A model is a set of rules that, when linked to a group, are used by Adaptive Risk Manager Online to evaluate the group member's activity at a specific Runtime.

1. On the Admin menu point to Models and then click List Models.

   The List Models page appears.

2. Enter the search criteria you want and click Run Query.

3. Click the name of the model you want to edit.

The Model Details page appears.

4. In the Rules list, click the name of the rule you want to add.

   You might, for example, select the rule LOCATION: In Country group. This rule checks whether a country is a member of a specific country group. This rule could be used to black list countries.

   The parameters of the rule appear in the Custom Rule area.

5. In the Rule Name box, enter the name you want for this instance of the rule template.

   When you add a rule to a model you are adding an instance of a rule template. You can then customize that instance.

6. Specify any settings needed for the pre-conditions.

   These settings determine if the rule will run.

7. To exclude a user group from the rule, click in the Excluded User Group and select the user group whose members you want this rule to ignore.

8. If the rule instance you are configuring is dependent on device identification accuracy, enter a score range for Device Risk Gradient to specify the amount of device identification risk with which you want the run the rule.

   For example, if the range is 0 to 400, the rule will only run if the device ID is greater than 60% positive.

9. If the rule instance you are configuring is dependent on IP location identification accuracy, enter a score range for Country, State, and City confidence factors to specify the amount of geo-location accuracy with which you want the run the rule.

   For example, if the range is 60 to 100 the rule will only run if the IP location is greater than 60% positive. This confidence factor is based on IP geolocation information provided by the IP location vendor.

10. Specify the threshold values you want for any conditions.

    For example, enter the group ID or number of seconds elapsed.

11. In the Actions Group list, select the group of actions you want triggered by this rule, if actions are required.

12. In the Alerts Group list, select the group of alerts you want sent if this rule is triggered.

13. Enter a rule score and weight value.

    You can change the weight value for a rule to instruct Adaptive Risk Manager Online to give more or less value to the total score.

14. Click Add.

    Adaptive Risk Manager Online adds this rule instance to the list of rules in the model.

3.1.8 Configuring a Rule Instance

When you add a rule to a model you are not actually adding the rule itself, but rather you are adding an instance of a rule template for which you can edit the parameters.

When you add rules to a model, you select the rule you want to activate and then provide the threshold values. By so doing, you instruct Adaptive Risk Manager Online

to activate a pre-defined set of actions, alerts and/or additional models when the threshold values are exceeded.

1. Display the Model Details page for the model you want to edit.
2. At the bottom of the page, click the name of the rule you want to edit in the list of rules that have already been added to the model.

   The parameters of the rule appear in the Custom Rule area.
3. To change the name, make the change you want in the Rule Name box.
4. Specify the threshold values you want for any conditions.

   For example, specify the group ID, list ID, number of seconds elapsed, or authentication status.
5. To change the actions group triggered by this rule, select the actions group you want from the Actions Group list.
6. To change the alerts group triggered by this rule, select the alerts group you want from the Alerts Group list.
7. You can change the weight or score by selecting a different value from the lists.
8. Click Save.

3.1.9 Examples of Configured Rules to Initiate Action and/or Alert

This section provides scenarios for setting up and configuring Adaptive Risk Manager to initiate an action or alert in response to different situations. Below are some examples of configured rule instances.

3.1.9.1 User is accessing from more than x devices within the specified time

To activate an action and/or alert if a user is accessing from more than x devices within the specified time:

1. On the Admin menu point to Models, and then click List Models.
2. Enter the search criteria you want and click Run Query.
3. On the List Models, click the name of the model you want to edit.
4. In the Rules list, select USER: Devices.

   The parameters for the rule are displayed in the Rule Instance Parameters area.
5. Click in the Rule Name box and type a name for the rule.
6. Click the Max number of devices box and enter a threshold number
7. Click in the Duration box and specify the number of seconds you want.

   For example, you might enter 120 seconds.
8. Click in the Action box and select the action group you want.

   For example, you might select an action group that includes Block so that Adaptive Risk Manager Online will prevent the login attempt.
9. Click in the Alert box and select the alert group you want.

   For example, you might select an alert level of High if a user logs in from more than 2 devices within 120 seconds.
10. Click Save.

3.1.9.2 Number of users using this device exceeds x for the past x seconds

To activate an action and/or alert if the number of users using this device exceeds x for the past x seconds:

1. On the Admin menu point to Models, and then click List Models.
2. On the List Models page, click the name of the model you want to edit.
3. In the Rules list, select DEVICE: Multiple Users.

   The parameters for the rule are displayed in the Rule Instance Parameters area.
4. Click in the Rule Name box and type a name for the rule.
5. Click in the Seconds Elapsed box and type the number of seconds you want.

   For example, you might enter 120 so that Adaptive Risk Manager Online will take some action if more than x users use this device in less than 120 seconds.
6. Click in the Maximum Number of Users Allowed box and type maximum number of users you want.

   For example, you might enter 2 as the maximum number of allowed users in 120 seconds.
7. Click in the Action box and select the action group you want.

   For example, you might select an action group that includes Block.
8. Click in the Alert box and select the alert group you want.

   For example, you might select an alert group that includes a High alert.
9. Click Save.

3.1.9.3 Number of login attempts with the given client exceeds x for the given time period

To activate an action and/or alert if the number of login attempts with the given client exceeds x for the given time period:

1. On the Admin menu point to Models, and then click List Models.
2. On the List Models page, select the model you want to edit.
3. In the Rules list, select USER: Client And Status.

   The parameters for the rule are displayed in the Rule Instance Parameters area.
4. Click in the Rule Name box and type a name for the rule.
5. Click in the Used Client and select the client you want.

   For example, you might select PinPad so that if the user enters the pin using a PinPad more than x times for the given period Adaptive Risk Manager Online will take some specified set of actions.
6. Click in the More than box and type maximum of attempts.

   For example, you might enter 5.
7. Click in the Duration Condition box and type the amount of time you want to evaluate.

   For example, you might enter 30 minutes as the time in which a user can use the PinPad 5 times before Adaptive Risk Manager Online takes specified action.
8. Click in the Action box and select the action group you want.

For example, you might select an action group that includes Challenge Questions.

9. Click in the Alert box and select the alert group you want.

   For example, you might select an alert group that includes a Medium alert.

10. Click Save.

3.1.9.4 IP is in the given country group

To activate an action and/or alert if the IP is in the given country group:

1. On the Admin menu point to Models, and then click List Models.
2. On the List Models page, click the name of the models you want to edit.
3. In the Rules list, select LOCATION: In Country Group.

   The parameters for the rule are displayed in the Rule Instance Parameters area.

4. Click in the Rule Name box and type a name for the rule.
5. Click in the Group ID box and select the group of counties you want.

   For example, you might want to select the group of countries that you created from which there have been many fraud attempts in the past three months.

6. Click in the Action box and select the action group you want.

   For example, you might select an action group that includes Block.

7. Click in the Alert box and select the alert group you want.

   For example, you might select an alert group that includes a Medium alert.

8. Click Save.

3.1.10 Editing a Model's Links

You can add and delete the User ID groups linked to a model as needed. Multiple User ID groups can be linked to a single model if required.

1. On the Admin menu point to Models, and then click List Models.
2. Enter the search criteria you want and click Run Query.
3. In the List Models page, click the name of the model you want to edit.

   The Model Details page appears.

4. Click the Group Linking tab.

   The Group Linking page appears.

5. Click in the Group Types box and select the User ID group type.
6. Click in the Group Name box and select the group you want to link.

   The User ID group's details appear in the Add Group area.

7. Click Add.

   The new link is added to list of linked User groups.

   To delete a linked group, select the check box next to the group you want to delete and then click Delete.

3.1.11 Specifying the Scoring of Rule Return Combinations

Oracle Adaptive Access Manager uses a system of numeric scoring to represent the risk level associated with a specific situation. Each rule has its own default score and weight. Most rules are Boolean and return a value of True or False; they either trigger the rule or they don't. Oracle Adaptive Access Manager uses the score and weight of each rule within a model to calculate the total model risk score.

The Manual Overrides page enables you to create outcomes based strictly on the combinations of rule triggers. You can specify a score, action group and alert group based on different rule return combinations or you can point to a nested model to further evaluate the risk. The rows of manual overrides evaluate from top to bottom, stopping as soon as a rule return combination is matched. Actions and alerts triggered by a manual override will be added to any actions and alerts triggered by individual rules.

3.1.11.1 Specify rule return combinations

To specify rule return combinations:

1. On the Admin menu point to Models, and then click List Models.
2. Enter the search criteria you want and click Run Query.
3. In the List Models page, click the name of the model you want to edit.

   The Model Details page appears.
4. Click the Manual Overrides tab in the lower half of the page.

   The Manual Overrides page appears.
5. Select the return value permutations you want for each rule in the first row.
6. In the Score/Model column, select score or model to specify whether the result should be a score or point to a nested model.
7. If you selected Score, in the right-hand column specify the score you want to assign to that combination.
8. If you selected Model, in the right-hand column, specify the model you want Adaptive Risk Manager Online to run to further evaluate the risk.
9. If you want to specify other rule return combinations, click Add New to add another row.
10. Repeat steps 4 through 7 for each rule return combination you want.
11. Click Save.

3.1.11.2 Delete a rule return combination

To delete a rule return combination:

1. Display the Manual Overrides page.
2. Select the check to the left of the combination you want to delete and click Delete.

3.1.11.3 Change the sequence of a rule return combination

To change the sequence of a rule return combination:

1. Display the Manual Overrides page.
2. To change the numbering sequence of a combination at once, click in the number field and type the new number then click Save.

3.1.12 Viewing a List of Models

On the List Models page, you can view a list of all models. The List Models page provides quick access to the Model Details page for any model.

1. On the Admin menu, point to Models, and then click List Models.

   The List Models page appears.

2. Enter the search criteria you want and click Run Query.
3. To filter the list by Model Type, select the type you want in the Model Type list and click Submit Query.
4. To filter the list by Model Runtime, select the Runtime you want in the Model Runtime list and click Submit Query.
5. To filter the list by status, click status you want in the Model Status list and click Submit Query.
6. To find a specific model, type the name of the model in the Model Name box and click Submit Query.
7. To view the details page for a model, click the Model Name.
8. To delete a model, select the check box to the left of the model name and then click Delete.

   You can also use Export Delete Script to export a delete script for the models you might want to delete in the future, and import the delete script later to delete the models if they are present.

3.1.13 Viewing and Changing Model Details

You can change model details when needed.

3.1.13.1 Modify details about a model

To modify details about a model:

1. On the Admin menu point to Models, and then click List Models.

   The List Models page appears.

2. Enter the search criteria you want and click Run Query.
3. Click the name of the model you want to view or modify.

   The Model Details page appears.

4. To change the model name, click in the Model Name box and type the name you want.
5. To change the description, click in the Description box and edit the description.
6. Click Save.

3.1.13.2 View details about the user groups linked to a model

To view details about the user groups linked to a model:

1. On the Admin menu point to Models, and then click List Models.

   The List Models page appears.

2. Enter the search criteria you want and click Run Query.
3. Click the name of the model you want.

The Model Details page appears.

4. Click the Group Linking tab.

   All of the user ID groups linked to the model are listed.

5. To delete a group, select the check box to the left of the group and then click Delete.

3.1.13.3 View details about the rules contained in a model

To view details about the rules contained in a model:

1. On the Admin menu point to Models, and then click List Models.

   The List Models page appears.

2. Enter search criteria and click Run Query.
3. Click the name of the model you want to modify.

   The Model Details page appears.

4. Click the Rules tab.

   The rules contained in the model are listed.

5. To view the rule details, click the name of the rule you want.

   The parameters appear in the Custom Rule area.

6. To view the Rule Details page, click the rule you want to see.
7. To view a complete description of the rule, click the link in the Description column.

3.1.14 Creating a Group of IP Ranges

You can create a group of IP ranges to use as a parameter in rules. For example, the result of a rule's execution might be to block a user if their IP address falls within a predefined range.

1. On the Admin menu point to IP Range, then click Create IP Range.

   The Create New IP Range page appears.

2. Click in the Label box and type a label for the range.
3. Click in the From box and type the starting IP range.
4. Click in the To box and type the ending IP range.
5. Type any description and notes you want.
6. Click Create.

   The IP Range Details page appears.

7. To change the label or IP range, click Modify.

3.1.15 Viewing a list of IP Ranges

This section provides procedures for viewing IP ranges.

3.1.15.1 View a list of IP ranges

To view a list of IP ranges:

1. On the Admin menu point to IP Ranges, and then click List IP Ranges.

   The List IP Ranges page appears.
2. Enter the search criteria you want and click Run Query.
3. To view IP range details, click the IP range Label you want.
4. To view details about the IP details, click the link in the From or To IP address column.

3.1.15.2 View details about an IP range

To view details about an IP range:

1. On the Admin menu point to IP Ranges, and then click List IP Ranges.

   The List IP Ranges page appears.
2. Enter search criteria and click Run Query.
3. Click the link in the Label column.

   The IP Details page appears.

3.1.16 Scenarios for Setting Up and Configuring Oracle Adaptive Risk Manager Online

This section provides scenarios for setting up and configuring Adaptive Risk Manager Online to initiate an action in response to different situations.

3.1.16.1 Rule Triggers

To create a rule to trigger if more than a set number of users log in from a location in a set amount of time:

1. Create a model to hold the rule you will add next.
2. Add the rule named Location: IP Max Users to the model.
3. Configure the seconds elapsed to 30.
4. Set max number of users to 3.
5. Create an Action group to be triggered if the rule returns a true result.
6. Add the Block Action to the Action Group.
7. Link User group and Model.

3.1.16.2 Ask Challenge Question

To create a rule forcing the system to ask a challenge question the first time a user attempts to log in from a new, unrecognized device:

1. Create a model to hold the rule you will add next.
2. Add the rule named Device: Device First Time For User to the model.
3. Create an Action group to be triggered if the rule returns a true result.
4. Add the Question/Answer action to the group.
5. Link User Group and Model.

3.1.16.3 Block Users

To create a rule blocking users following a certain number of login failures:

1. Create a model to hold the rule you will add next.
2. Add the rule named User: Multiple Failures to the model.
3. Configure rule to the maximum number of failed login attempts for a given period.
4. Create Action group.
5. Add the Block action to the group.
6. Link User Group and Model.

3.2 Best Practices for Adding or Adjusting Models/Rules When the Solution is Up and Running

To create new rules/models and tune them without impacting customers:

1. Develop the new rule using Adaptive Risk Manager Offline.
2. Test the rule to ensure it is functioning as expected by running predictable data through it using Adaptive Risk Manager Offline.
3. When you are satisfied that the model is functioning as expected, migrate the model in pre-production where performance testing can be run.

   This is an important step since the new rule template and/or model can potentially have a big performance impact. For example, if you define a new model to check that a user was not using an email address that had been used before (ever). If you have over 1 billion records in your database, performing that check against all the records for every transaction will have a great impact on performance. Therefore, testing the model under load is important.
4. Only when you are satisfied that your new rule/model is functioning as expected and does not adversely affect performance should it be migrated into production.

3.3 How Models and Rules are Used to Enable Authenticators

This section introduces the basic pre-auth and post-auth models.

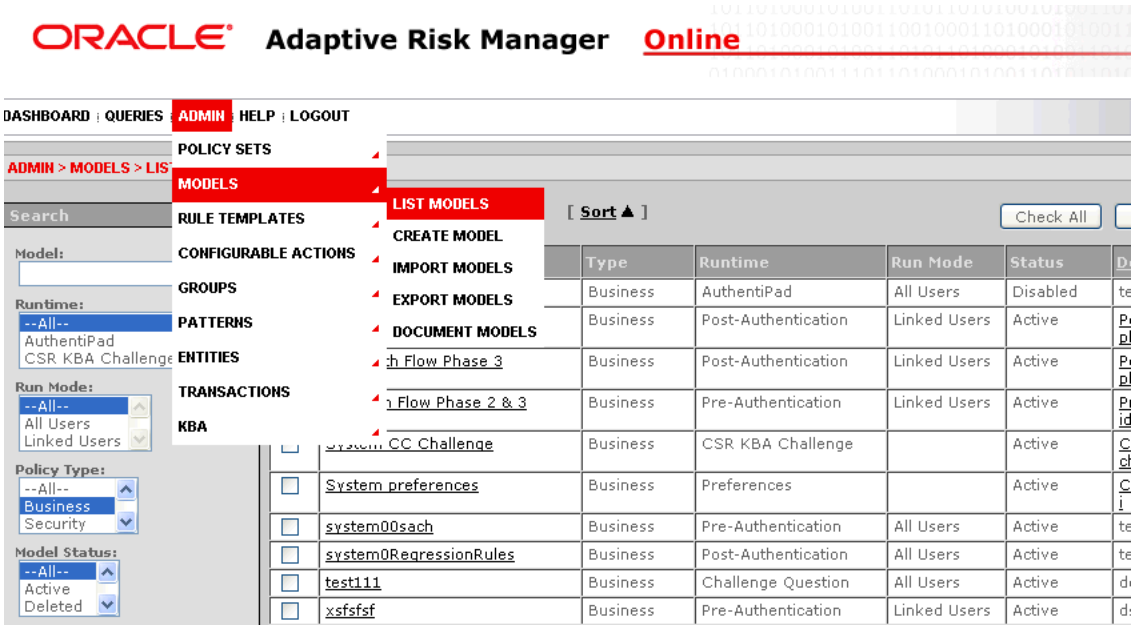
3.3.1 Basic Pre-Auth Model

3.3.1.1 Basic Pre-Auth Model Rules

In Adaptive Strong Authenticator, the Pre-Auth model will be executed after the user enters a User ID and before the password page is displayed. This model will select the KeyPad or TextPad authenticators for display.

To view the two rules that are in this model:

1. On the Admin menu point to Models, and then click List Models.

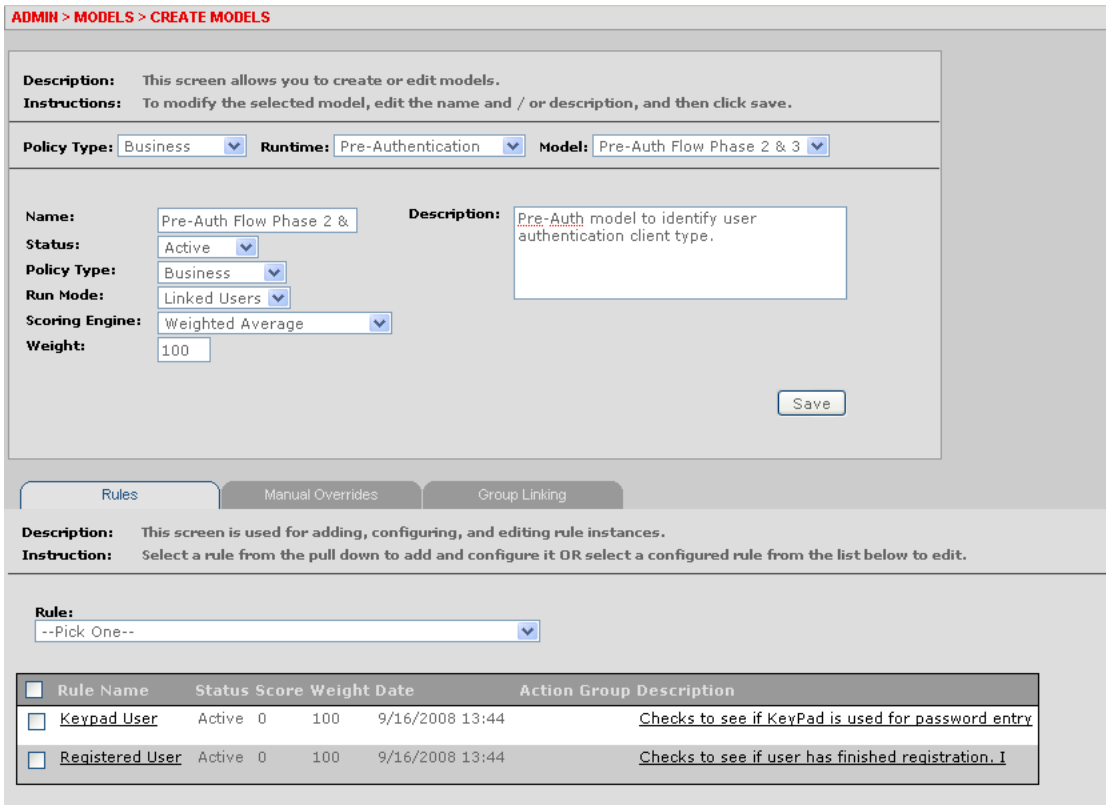


2. For the Policy Type filter, select Business and click Run Query.
3. Click the Pre-Auth Flow Phase 2 & 3 link.

   The Create Models page appears.

   On the Rules tab at the bottom of the page, the following rules are displayed.

   - Keypad User
   - Registered User



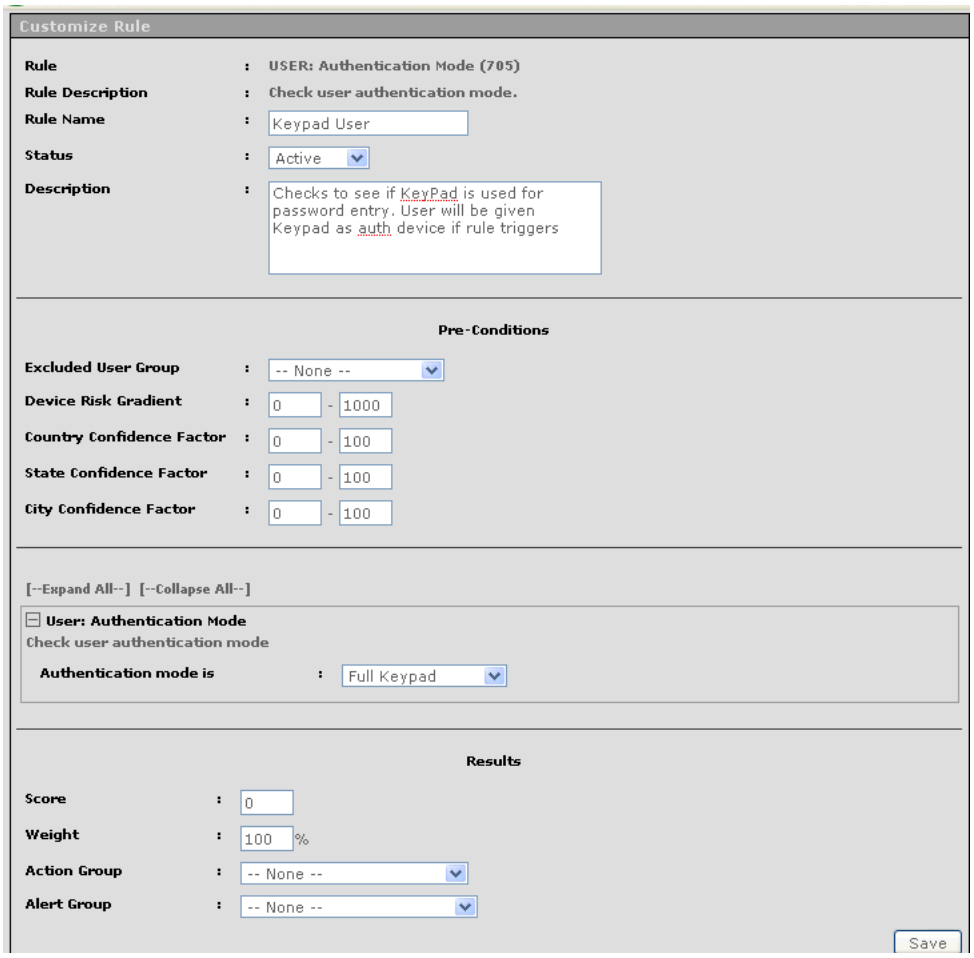
The rules that are defined are shown in the table below.

Rule	Template	Usage
Keypad User	USER: Authentication Mode	User will be given Authentication Pad
Registered User	USER: Account Status	When user has completed registration

3.3.1.2 Pre-Auth Model KeyPad User Rule

A rule instance is created from a rule template by editing/configuring the values and attaching it to a model. The Keypad User rule determines if a keypad is required to be rendered to a user.

Click Keypad User in the Rule Name column.



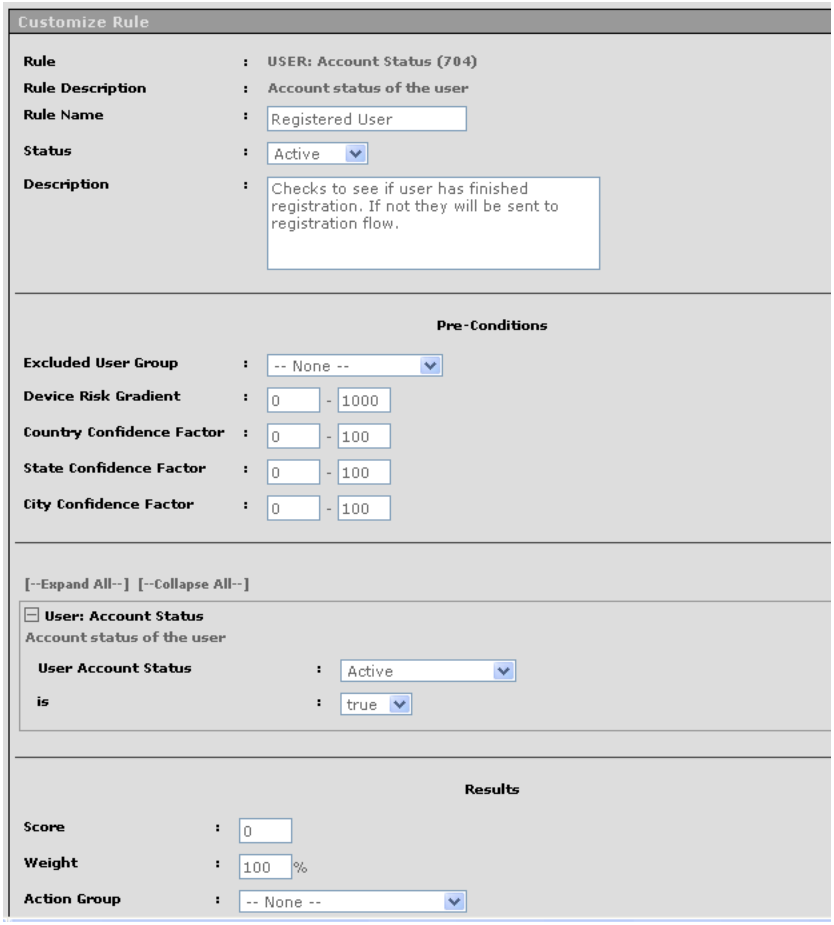
The Keypad User rule instance is derived from the rule template, USER: Authentication Mode. This rule template allows you to determine which mode of authentication has been assigned to a user (the rule condition) and then trigger an Action or Alert based on the rule.

For example, the mode is Full Keypad, which means if the user has already been assigned the full keypad authentication pad, perform the Action Group and/or Alert Group operation. In this case, both the Action and Alert Groups are empty, but you can set them to any action/alert depending on the requirement.

3.3.1.3 Pre-Auth Model Registered User Rule

The Registered User rule determines if a user has been enrolled in the Oracle Adaptive Access Manager system for personalization.

1. Scroll down on the Customize Rule page and click the Registered User link.



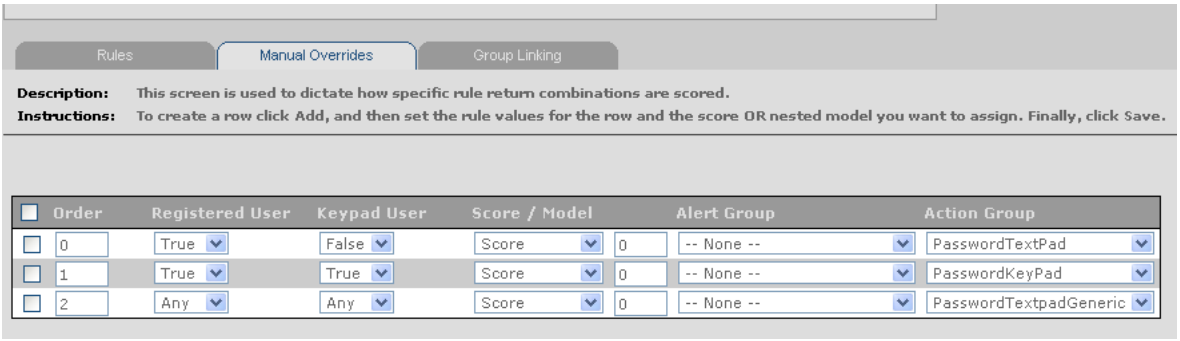
The Registered User rule is the rule instance derived from the rule template, USER: Account status where you can set conditions such as active, pending activation, disabled on which you can perform action and generate alerts.

2. In the section underneath Pre-Conditions, set the User Account Status to Active and the "is" field to "true."

3.3.1.4 Pre-Auth Model Manual Overrides

Generate the final Pre-Auth model by combining the two rules using the Manual Override feature.

Click the Manual Overrides tab. It is the tab in between the Rules tab and the Group Linking tab.



In the Manual Overrides screen, the following conditions are set based on the rules that are triggered. The rules used in the model are represented by the column names.

- True: The rule is triggered
- False: the rule is not triggered
- Any: Ignore the rule whether or not it triggers

Conditions are read in the order of 0, 1, 2, n…

If a rule condition fires, subsequent rules in the same list are not invoked. For example, if condition 1 fires, condition 2 is not processed.

1. If the Registered User rule is triggered (true), and the Keypad User rule is not triggered (False), then, generate a score of "0" and action (display) PasswordTextpad.
2. If the Registered User rule is triggered (true), and the Keypad User rule is triggered (True), then generate a score of "0" and action (display) PasswordKeyPad
3. If neither conditions are met, then action (display) PasswordTextPadGeneric authenticator

For the user to be tagged "Registered User" he must first go through the process of registration where he will select his personalized image.

3.3.2 Basic Post-Auth Model

3.3.2.1 Basic Post-Auth Model Rules

In Adaptive Strong Authenticator, this model is executed after the user enters the password and clicks submit. This model allows the user to register his personalized image and his security questions.

1. On the Admin menu point to Models, and then click List Models.
2. For the Policy Type filter, select Business and click Run Query.
3. Click the Post-Auth Flow Phase 2 link.

   The Create Models page appears.

   On the Rules tab at the bottom of the page, the following rules are displayed.

   - Question Registered - Does this user have security questions registered?
   - Registered User - User has completed registration and personalization.

- Unregistered User - User has not yet completed registration and personalization

  The rules that are defined are shown in the table below.

Rule	Template	Usage
Question Registered	USER: Question Status	When user finished question registration
Registered User	USER: Account Status	When user has completed registration and personalization
Unregistered User	USER: Account Status	When user has not yet completed registration and personalization

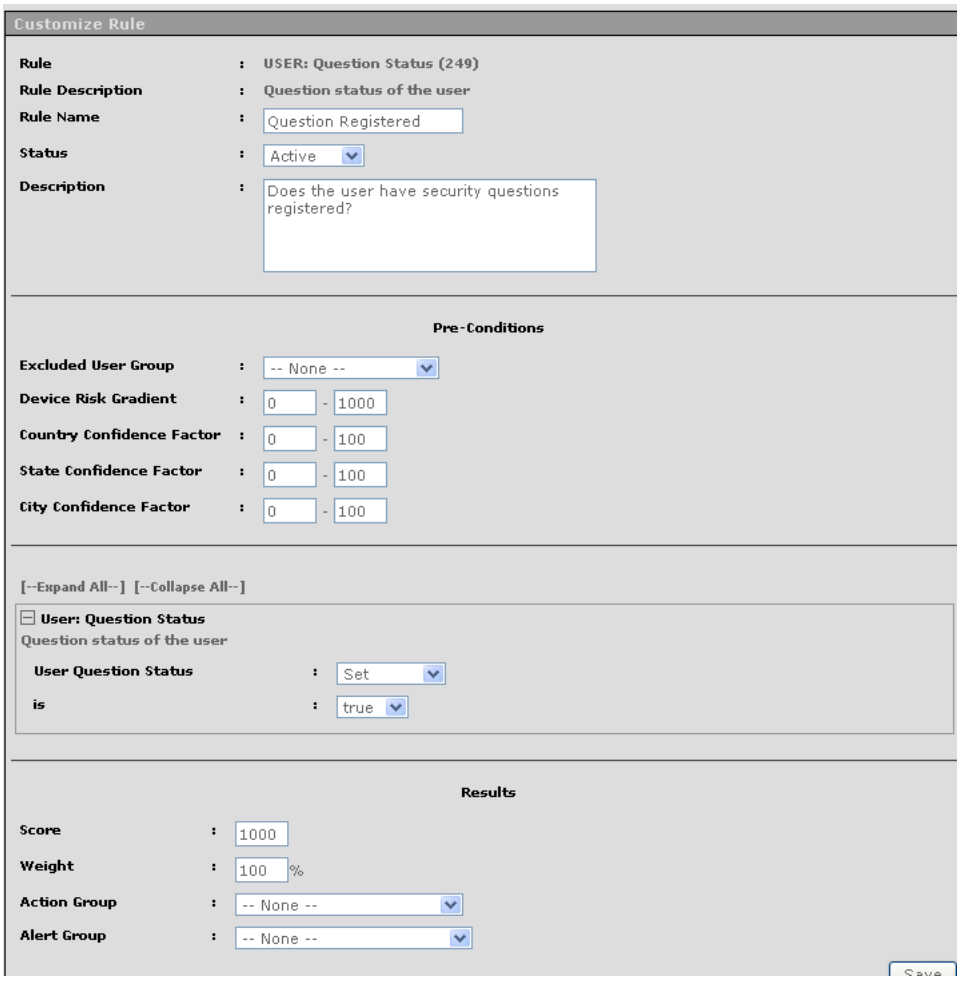
3.3.2.2 Post-Auth Model Question Registered Rule

A rule instance is created from a rule template by editing/configuring the values and attaching them to a model. This rule instance checks if questions are set for the user. The manual override in model will decide which action to take based upon combination of rule results

Click Question Registered in the Rule Name column.

The Question Registered rule instance is derived from the rule template, USER: Question Status. This rule template allows you to determine if User Question Status is set or not and whether the status is true or false.

For example, if User Question Status is set to true, then perform an action/alert and assign appropriate score and weight. In this example, both Action and Alert groups are empty.



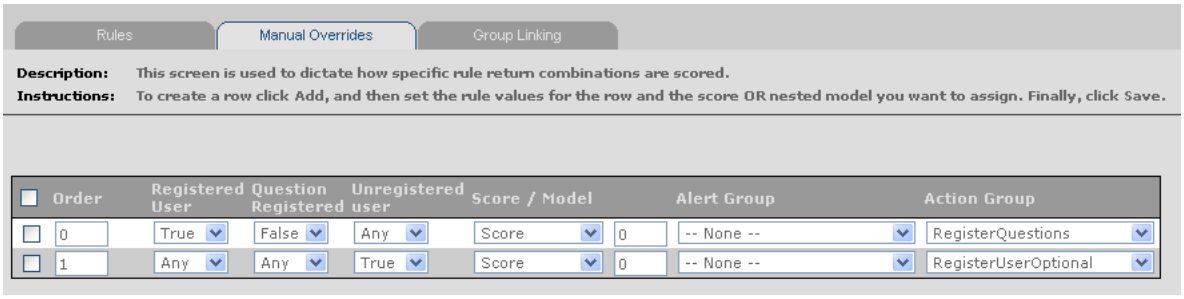
3.3.2.3 Post-Auth Model Manual Overrides

Generate the Post-Auth model by combining the two rules using the Manual Overrides feature. The Unregistered User and the Registered User rule configuration is the same as the configuration explained in the "Pre-Auth Model Registered User Rule" section.

Click Manual Overrides

In the Manual Overrides screen, the following conditions are set based on the rules that are triggered. The rules used in the model are represented by the column names.

- True: The rule is triggered
- False: the rule is not triggered
- Any: Ignore the rule whether or not it triggers



The above conditions are read in the following order of 0 to 1:

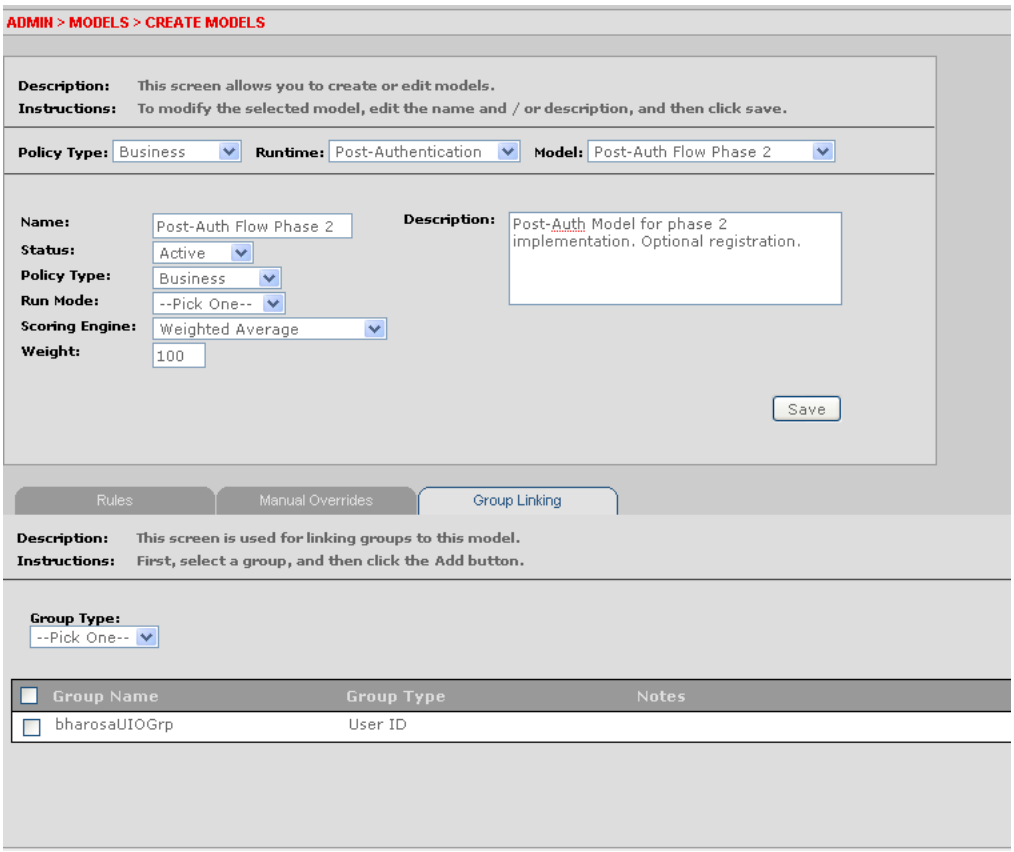
1. If the Registered User rule is triggered (True) and the Question Registered rule is not triggered (False), generate a score of "0" and action (display) Register Questions page. The Unregistered User rule is ignored.
2. If the Unregistered User rule is triggered (True), generate a score of "0" and action (display) RegisterUserOptional page. RegisterUserOptional allows a user to opt in or out of a personalized image.

3.3.3 Link Groups to Models

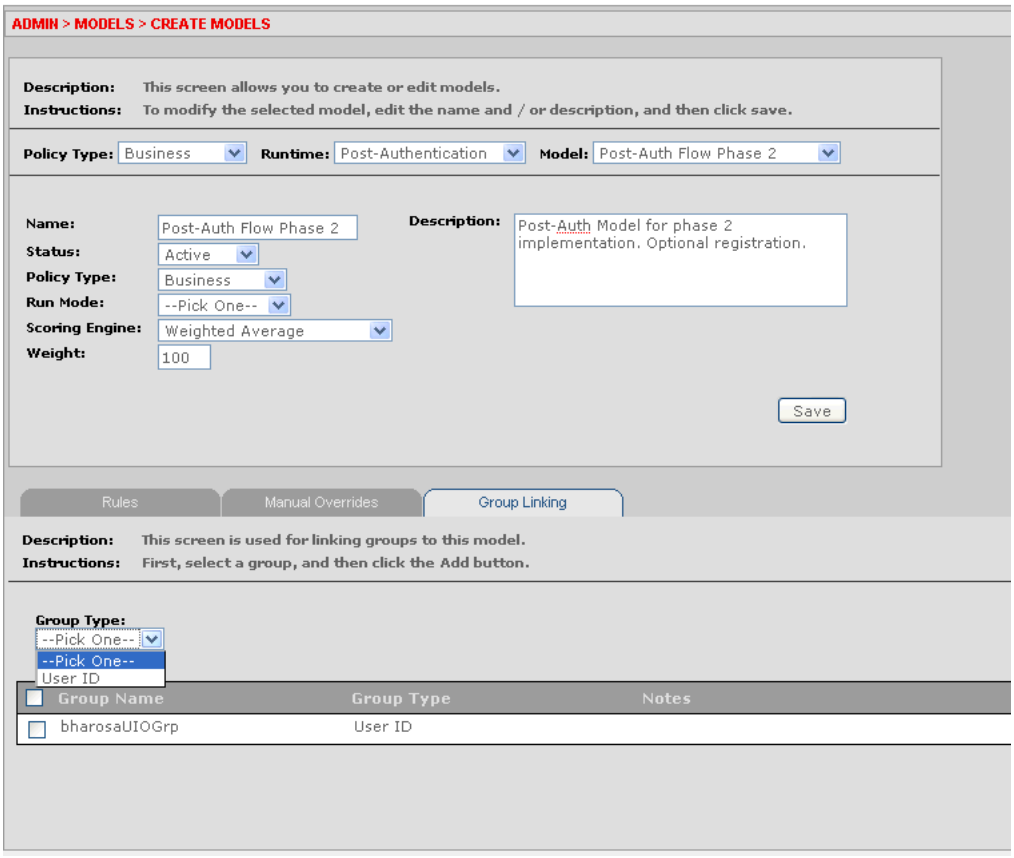
Once the models and rules are configured, they are linked to groups, which enables them to execute/run for that set of users within the linked group.

Group linking for Pre- and Post-Auth models is shown below.

1. Click Group Linking.



2. From Group Type, select User ID.



3. From the Group list, select a group and click Add. For example, bharosaUIOGrp.
4. For the Pre-Auth, perform the same group linking steps as the Post-Auth.

These models are now configured to execute for users who are members of the group you selected, for example, bharosaUIOGrp.

If you are using the standard base models, by group linking your user group (BharosaUIOGrp by default) to the Phase2/Phase3 pre-authentication and post-authentication models, new users will be asked to register their challenge questions.

4

Rule Templates and Conditions

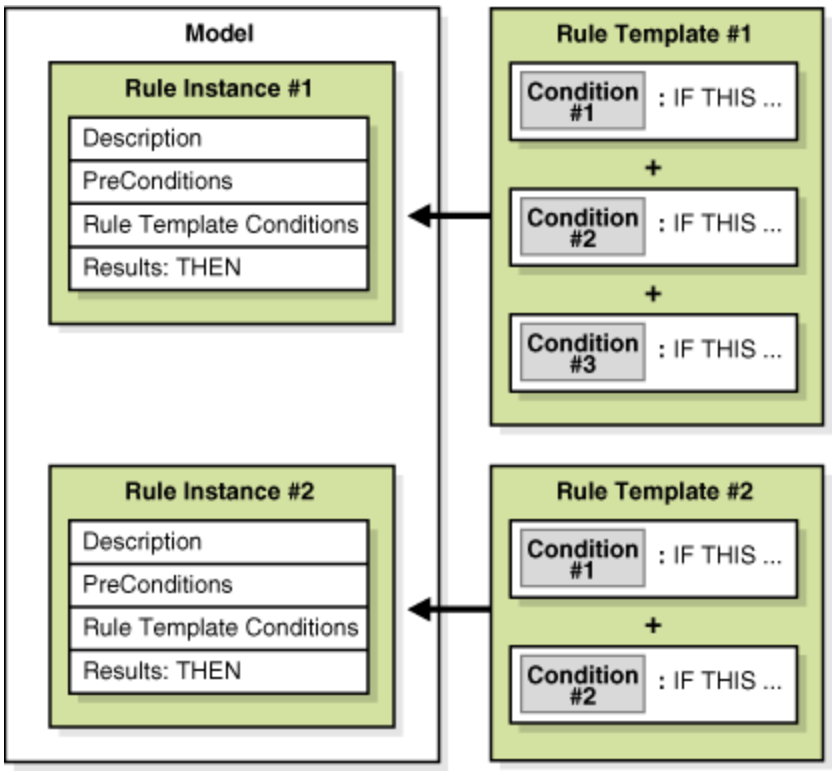
This chapter provides information about creating and editing rule templates, using the rules template editor, managing conditions, and importing and exporting rules and conditions.

4.1 How Rule Templates and Conditions Work

Rule conditions are the building blocks for constructing rule templates and make the rule-related functions in Oracle Adaptive Access Manager available to the client. Rule conditions consist of references to various Oracle Adaptive Access Manager objects, APIs (functions), and parameters that are used to evaluate the risk. The parameters could be Runtime variables, capture Runtime data, time, username, authentication, IP, and so on.

The rule template forms the basis for creating a rule instance. Adding condition instances to rule templates allow you to create the template you need for your use cases. Rule templates must have at least one condition.

Conditions in the rule template are evaluated sequentially. Subsequent conditions are evaluated only if the current one was evaluated to be true. In other words, the evaluation stops when a condition is evaluated to be false. For the rule to be triggered all the conditions that constitute the rule need to be evaluated to true; if any of the conditions is evaluated to false, the rule is evaluated to false, and the rule does not trigger.



4.2 Before You Begin

Oracle Adaptive Access Manager includes a library of preconfigured conditions. For a list of these conditions, refer to Appendix A, "Conditions Reference." Conditions cannot be modified. Before you can use conditions, you must import oaam_rule_conditions.zip, which contains all conditions that come standard with the product, into your system.

To import the oaam_rule_conditions.zip:

1. On the Admin menu, point to Rule Templates, point to Conditions, then click Import Conditions.
2. Click Browse and locate oaam_rule_conditions.zip.
3. Click Import.

All the conditions are imported into the server.

4.3 Managing Conditions

This section contains instructions on

- Viewing a List of Conditions
- Viewing Details of a Condition
- Exporting and Importing Conditions
- Deleting a Condition

You can import, export, and delete conditions as necessary.

4.3.1 Viewing a List of Conditions

To view a list of available conditions:

1. On the Admin menu, point to Rule Templates, point to Conditions, then click List Conditions.

   The List Conditions page appears.

2. To filter the list by type, click in the Type box and select the type you want. Then click Run Query.

   By default there are 7 types of rule conditions in Adaptive Risk Manager:

   - Device
   - Device ID Conditions
   - In Session
   - Location
   - System Conditions
   - User
   - User Device ID Conditions

   The type of condition identifies the type of Oracle Adaptive Access Manager API that will be used at Runtime. However, system conditions are special conditions that do not necessarily adhere to using a type of Oracle Adaptive Access Manager API.

3. To filter the list by condition name, click in the Condition Name box and type in the name or part of the name for the condition you want. Then click Run Query.

   The search is case sensitive and it does not take special characters.

4. After filtering the list of conditions, you can sort them by clicking Condition Name, Sort, or Description.

   Clicking the Condition Name heading will sort all the condition names in ascending or descending order. Clicking the Description heading will sort all the condition descriptions in ascending or descending order. The Sort option sorts the listed conditions by condition names or by condition descriptions in ascending or descending order depending on the last sort.

4.3.2 Viewing Details of a Condition

To view the details of a condition

1. On the Admin menu, point to Rule Templates, point to Conditions, then click List Conditions.

   The List Conditions page appears.

2. Click the name of the condition you want.

   The Condition Detail page appears.

The page contains a Delete button and non-editable details of the condition.

The following information is presented:

- Condition ID: the condition ID
- Condition Name: the name of the condition

- Status: Active or Disabled.
- Value Type: Type of condition.
- Description: the description given to the condition.
- Parameters: the parameters of the condition.

4.3.3 Exporting and Importing Conditions

You can export and import rule conditions.

To export a condition

1. On the Admin menu, point to Rule Templates, point to Conditions, then click List Conditions.
2. Select the check box next to the condition you want to export.
3. Click Export.

To import a condition

You can import a collection of 0 or more conditions through a zip file or a single condition through an .xml file.

1. On the Admin menu, point to Rule Templates, point to Conditions, then click Import Conditions.
2. Click Browse and locate the file.
3. Click Import.

Caution: If you import a condition that already exists in the system, the incoming condition will overwrite the existing condition. Changing the condition affects the Rules and Models that use the condition.

To export a delete script

1. On the Admin menu, point to Rule Templates, point to Conditions, and click List Conditions.

   The List Conditions page appears.
2. Click the check box next to the condition or conditions you want to delete.
3. Click Export Delete Script.

Export Delete Script exports a delete script for the conditions that you have selected. You can import this script later to delete the conditions in the application if they are present.

4.3.4 Deleting a Condition

You can delete conditions by using:

- by using the Delete button on the List Conditions page.
- by using the Delete button on the Condition Detail page.
- by importing a delete script.

Note: If rule templates are using the condition, deleting it will affect the rule templates and models that use it.

To delete a condition using the Delete button on List Conditions

1. On the Admin menu, point to Rule Templates, point to Conditions, and click List Conditions.

   The List Conditions page appears.

2. Click the check box next to the condition or conditions you want to delete.
3. Click Delete.

To delete a condition using the Delete button on Condition Detail

1. On the Admin menu, point to Rule Templates, point to Conditions, and click List Conditions.

   The List Conditions page appears.

2. Click the condition you want to delete.

   The Condition Detail page appears.

3. Click Delete.

To delete a condition by importing a delete script

Import a delete script that you created earlier (with Export Delete Script) to delete conditions in the application if they are present.

1. On the Admin menu, point to Rule Templates, point to Conditions, then click Import Conditions.
2. Click Browse and locate the file.
3. Click Import.

4.4 Managing Rule Templates

The rules templates contain the rules definition of the parameters that can be configured from the web interface. The rules are loaded into the database using the import process.

4.4.1 Viewing a List of Rule Templates in the System

1. On the Admin menu, point to Rule Templates and then click List Rule Templates.

   The List Rule Templates page appears.

2. To filter the list by type, click in the Rule Type box and select the type you want and click Run Query.

   By default there are 6 types of rule templates in Adaptive Risk Manager:

   - Device
   - Device ID Rules
   - In Session
   - Location

- User
- User Device ID Rules

The type of rule template identifies the type of Oracle Adaptive Access Manager API that will be used at Runtime.

3. To filter the list by status, click in the Rule Status box and select the status you want and click Run Query.
4. To filter the list by rule template name, click in the Rule Name box and type in the name or part of the name for the rule template you want. Then click Run Query.

   The search is case sensitive and it does not take special characters.
5. After filtering the list of rule templates, you can sort them by clicking Condition Name, Sort, or Description.

   Clicking the Rule Name heading will sort all the rule template names in ascending or descending order. Clicking the Description heading will sort all the rule template descriptions in ascending or descending order. The Sort option sorts the listed rule templates by rule template names or by rule template descriptions in ascending or descending order depending on the last sort.
6. To edit a rule template, click the wrench icon next to the rule template you want.

   The Create Rule Template page appears.

4.4.2 Creating and Editing a Rule Template

The Create Rule Template page provides the ability to create and edit rule templates for your own specific set of needs and requirements.

To create or edit a rule template:

1. On the Admin menu, point to Rule Templates and then click Create Rule Templates.

   The Create Rule Template page appears.

   Note: you can also access the Create Rule Template page for editing by listing the rule templates, and then clicking the wrench icon next to the rule template you want to edit. In this case, you can skip steps 2 and 3.
2. Click in the Rule Type box and select the type of rule you want.

   The Rule field appears.
3. To create a new rule template, select Create New Rule Template. To edit an existing rule template, select the rule template you want.
4. In the Rule Name box, enter or edit the rule name.

   If you are creating a new rule template, it is recommended that you use a prefix such as Device, Location, or User to identify the template as a particular type.
5. In the Description field, enter or edit the description of the rule template.
6. Click the Status box and select the status you want: Active or Disabled.

   If status is changed to disabled, the rule is disabled and cannot be added to a model. A Model that already contains the rule will not be affected and will continue to function as before.
7. Click in the Condition box and select the condition you want to add to the rule.

Oracle Adaptive Access Manager filters the list of conditions displayed based on the selected rule type.

The Add Condition box appears to the right of the list of conditions. The box displays the name and description of the condition.

8. To edit the parameters for your rule template, click in the appropriate field in the Add Condition box and make the changes you want.
9. In the Add Conditions box, click Add.

   The same condition can be added more than one time.
10. To change the order in which the conditions are evaluated, click the Order box and select the order you want.
11. Repeat steps 7 through 10 for each condition you want to add to the rule template.
12. Click Save.

    The rule template is created.

    An error message appears if a template with the same name already exists.

4.4.3 Viewing Details of a Rule Template

To view details of a rule template:

1. On the Admin menu, point to Rule Templates and then click List Rule Templates.

   The List Rule Templates page appears.
2. Click the name of the rule template you want.

   The Rule Templates page appears.

The Rule Templates page displays the following information:

- Rule Id
- Rule Name
- Rule Status
- Rule Type
- Description
- Notes

From the Rule Templates page, you can also modify the rule description, status, and notes; delete the rule template; and access the Create Rule Template page to edit the rule template.

You can edit the Description field. The description will contain one line of information that people using Adaptive Risk Manager will see. It will appear in the Description column on the List Rule Templates page and the Customize Rule box when you add that rule to the model.

You can add notes for the rule template. Notes allow the administrator to add detailed information about the rule template. This information will only appear in the Rule Detail page.

A rule of thumb is that if you have one line of information about the rule template, store the information in Description so that other people using Adaptive Risk Manager can see it, and that if you have detailed information, store it in Notes.

You change the rule status of the rule template. If the rule status is changed from Active to Disabled, the rule is disabled and cannot be added to a model. A Model that already contains the rule will not be affected and will continue to function as before.

4.4.4 Deleting a Condition Instance from a Rule Template

You can delete a condition, but a rule template requires a minimum of one condition to function.

If a rule template includes only one condition, that condition cannot be deleted.

If a rule template includes more than one condition, you can delete all of the conditions except one (with least order number).

To delete a condition from a rule template:

1. On the Admin menu, point to Rule Templates and then click List Rule Templates.

   The List Rule Templates page appears.

2. Click the wrench icon next to the name of the rule template you want.

   Alternatively, you can click the rule template name, and then the Edit button on the Rule Templates page.

   The Create Rule Template page appears.

3. Click the check box next to the condition you want to delete.

   The message appears: "Are you sure you want to delete the selected row(s)?"

4. Click OK.

4.4.5 Deleting a Rule Template

When you delete a rule template any active instances of that rule will also be deleted which may cause unwanted results. Deleting a rule template does not delete the actual conditions.

You can delete rule templates in three ways:

- by using the Delete button on the List Rule Templates page.
- by using the Delete button on the Rule Templates page.
- by importing a delete script

Deleting from the Rule Templates page does not offer you the option of exporting the selected rows before deleting.

To delete a rule template from the List Rule Templates page

1. On the Admin menu, point to Rule Templates and then click List Rule Templates.

   The List Rule Templates page appears.

2. Click the check box next to the rule templates you want to delete.

3. Click Delete.

   The message appears: "Deleting a rule will cascade delete the rule profile maps if the rule is linked to a profile. Are you sure you want to delete the selected rows?"

4. Click OK.

   The option appears, "Do you wish to export the selected rows before deleting."

5. Click OK if you want to save the selected rows to disk or click Cancel.

To delete a rule template from the Rule Templates page

1. On the Admin menu, point to Rule Templates and then click List Rule Templates.

   The List Rule Templates page appears.

2. Click the name of the rule template you want.

   The Rule Templates page appears.

3. Click Delete.

   The message appears: "Do you want to cascade delete the rule profile maps if the rule is linked to a profile?"

4. Click OK.

   The message appears: "Are you sure you want to delete this rule permanently from the database."

5. Click OK.

To delete a rule template by importing a delete script

1. On the Admin menu, point to Rule Templates and then click Export Rule Templates.

   The Export Rule Templates page appears.

2. Click the check box next to the rule templates you want to delete in the future.

3. Click Export Delete Script.

   The option appears, "Do you wish to export the selected rows before deleting."

4. Click OK.

   Export Delete Script exports a delete script for the rule templates that you have selected. You can import this script later to delete the rule templates in the application if they are present.

4.4.6 Exporting and Importing a Rule Template

You can export and import rule templates.

When you export a rule template, the exported rule template includes the corresponding conditions.

To export a rule template

1. On the Admin menu, point to Rule Templates and then click Export Rule Templates.

   The Export Rule Templates page appears.

2. Enter the search criteria you want and click Run Query.

3. Select the check box next to each rule template you want to export.

4. Click Export.

5. Click OK to the confirmation.

6. To open a rule template, click Open With and select the application you want to use.

7. To save the template to disk, click Save To Disk.
8. Click OK.

To import a rule template

1. On the Admin menu, point to Rule Templates and then click Import Rule Templates.

   The Import Rule Templates page appears.
2. Click Browse and locate the rule template you want to import.
3. Click Import.

   The imported template appears in the List of Rule Templates.

Caution: If you import a rule template that already exists in the system, the imported template will overwrite the existing template. The accompanying conditions will also overwrite the conditions already in the server.

5

Configurable Actions

Oracle Adaptive Access Manager provides Configurable Actions, a feature which allows users to create new supplementary actions that are triggered based on the result action and/or based on the risk scoring after a Runtime execution.

This chapter provides an overview on configuring a Configurable Action and instructions on how to define, view, edit, and delete a Configurable Action, and on how to associate Configurable Actions to a Runtime.

5.1 Before You Begin

To use the Configurable Actions feature, ensure that the dynamicactions.enabled property is set to true.

5.2 Configuring a Configurable Action

Configuration of Configurable Actions involves the following tasks:

1. Determining what Configurable Actions have to be added to which Runtime and the pre-conditions for executing those Configurable Actions.

   An example of a Configurable Action is when an email is sent to a user whenever a Runtime execution returns "block" as an action in the result. In this case, "Send Email" is the Configurable Action and "block" is the pre-condition. Similarly, there could be Configurable Actions that can be based on a "risk score" as the pre-condition.

2. Making sure the Configurable Action definitions are configured in the Adaptive Risk Manager database.

   A user can see the list of available Configurable Actions before adding a new one. The Configurable Action definition would have been added into the database when the user created the definition using the "Define New Action Template" screen.

3. Developing and deploying custom Configurable Actions if the existing Configurable Actions are not sufficient. See the *Oracle Adaptive Access Manager Developer's Guide* for details on developing a Configurable Action.

   Although some Configurable Actions are provided with the product, you may have to develop custom Configurable Actions for your particular requirements.

4. Using Adaptive Risk Manager to associate the Configurable Actions to the Runtime.

5.3 Defining a New Action

To define a new action:

1. On the Admin menu, point to Configurable Actions, click Action Templates, and choose Action Templates.
2. In the Action Name field, enter a name for the action.
3. In the Java Class Name field, enter the fully qualified classpath of the Configurable Action.

   You will have created the Java Class during the creation of the Configurable Action. For information on creating a Configurable Action, refer to the *Oracle Adaptive Access Manager Developer's Guide*.

   An example of a Java Class is com.bharosa.vcrypt.tracker.dynamicactions.EmailAction.
4. Click Load Parameters.

   Oracle Adaptive Risk Manager obtains the list of parameters and displays the names, labels, types, and values.

   Examples of parameters are shown in the table below.

Name	Label	Type	Value
Recipient Email Address	To:	String	<value>
Sender Name	Name:	String	<value>
Sender Email Address	From:	String	<value>
Reply-to Email Address	Reply-to:	String	<value>
Mail Subject	Subject:	String	<value>
Mail Body	Subject:	String	<value>

5. Enter values for the parameters.
6. In the Description field, enter a description of the action.
7. In the Notes field, enter any notes you want.
8. Click Save.

5.4 Adding a Configurable Action to a Runtime

To add a Configurable Action to a Runtime:

1. From the Configurable Action item of the Admin menu, select Configured Actions, and then Create Action Instances to associate Configurable Actions to the Runtime.
2. Choose the Runtime to associate the Configurable Actions to.
3. Click Load Actions.
4. Choose the required Configurable Action from the list.
5. Choose the execution type: "Synchronous" or "Asynchronous."

   Synchronous actions are executed in the order of their priority in the ascending order. For example, if the user wants to create an agent case and then send an

email with the case ID, he would choose synchronous actions. Synchronous actions will trigger/execute immediately.

Synchronous actions can also be used to pass/share data across the configurable actions. This is useful when developing custom configurable actions. Please refer to "Configurable Actions" in the *Oracle Adaptive Access Manager Developer's Guide* for details.

Asynchronous actions are queued for execution and will be executed based on their priority but not in any particular sequence. For example, if the user wants to send an email or perform some action and does not care about executing it immediately and is not interested in any order of execution, he would choose asynchronous actions.

6. Enter values for all the parameters related to the action.
7. Enter the values for the pre-conditions.

   A pre-condition could be either a score or an action or both. These will be compared against the values returned by the Rule Engine for the selected Runtime while defining configurable action. For example, the pre-condition may be that if the Rules Engine returns "Allow" as the action, the Configurable Action will be executed. Another example would be, if the Rules Engine returns a score between "x" and "y," the Configurable Action will be executed.

   Typical actions returned by the Rules Engine are "Allow," "Block," "PasswordTextpad," and others.

   A typical score returned by the Rules Engine is a numeric value between 0 and 1000.
8. Add any other required Configurable Actions to the Runtime by repeating steps 4 to 7.

   Administrators can specify one or more Configurable Actions for a Runtime.
9. Save the changes.

5.5 Viewing Configurable Actions

1. From the Configurable Action item of the Admin menu, select Configured Actions, and then List Action Instances to see the list of Configurable Actions available.
2. Select a Runtime to see all the Configurable Actions for that Runtime or select All to see all Configurable Actions for the Runtimes.
3. View details of the Configurable Action you want and make sure the parameters are properly defined and that the Java class is valid.

5.6 Editing an Existing Configurable Action

To edit an action:

1. On the Admin menu, point to Configurable Action, click Action Templates, and then Action Templates.
2. Click an existing action definition.
3. Make changes to the action.
4. Click Save.

5.7 Deleting an Existing Configurable Action

To delete an action:

1. On the Admin menu, point to Configurable Action, click Action Templates, and then Action Templates.
2. Click an existing action definition.
3. Click Delete.

If an action is associated with a Runtime, you will not be able to delete it.

5.8 Out-of-the-Box Configurable Actions

The following configurable actions are available out of the box:

- CaseCreationAction - Can be used to create a case
- EmailAction - Can be used to send an email

Before these configurable actions can be configured for Runtimes, the definitions of these should be added.

> **Note:** To use system provided configurable actions, you must import the configurable action definition from the oaam_init directory.

5.8.1 Defining CaseCreationAction

To define CaseCreationAction:

1. Log in as a Rule Administrator.
2. On the Admin menu, point to Configurable Actions, click Action Templates, and choose Action Templates.
3. In the Action Name field, enter a name for CaseCreationAction.
4. Enter the java class name as

   ```
   com.bharosa.vcrypt.tracker.dynamicactions.impl.CaseCreationAction
   ```

5. In the Description field, enter a description for CaseCreationAction.
6. In the Notes field, enter any notes you want.
7. Click Load Parameters.
8. For the "Case Type" parameter, enter 1 for "CSR Case", 2 for "Agent Case".
9. For the "Severity" parameter, enter 1 for "Low", 2 for "Medium", 3 for "High."
10. Enter a value for the "Case Description" that should be set while creating the case.
11. Enter the userId for "Case Creator UserId". Make sure that userId has a proper role and access permissions for creating the case.

5.8.2 Defining EmailAction

To define EmailAction

1. Make sure the java mail library related jars are in the WEB-INF\lib directory of the Adaptive Risk Manager application.

2. Make sure the following properties are properly set in the Adaptive Risk Manager application.
   - mail.smtp.host > SMTP Host Address
   - mail.smtp.user > SMTP UserId
   - mail.smtp.password > SMTP password
   - mail.smtp.auth > true if SMTP server requires authentication, false otherwise
3. Log in as a Rule Administrator.
4. On the Admin menu, point to Configurable Actions, click Action Templates, and choose Action Templates.
5. Enter the action name for EmailAction.
6. Enter the java class name as

   ```
   com.bharosa.vcrypt.tracker.dynamicactions.impl.EmailAction
   ```

7. In the Description field, enter a description for EmailAction.
8. In the Notes field, enter any notes you want.
9. Click Load Parameters.
10. Enter appropriate values for the parameters:
    - Recipient Email Address
    - Sender Name
    - Sender Email Address
    - Reply-to Email Address
    - Mail Subject
    - Mail Body

5.8.3 Defining Add Item to List Action

To define "Add Item" to List Action:

1. Log in as a Rule Administrator.
2. On the Admin menu, point to Configurable Actions, click Action Templates, and choose Action Templates.
3. In the Action Name field, enter a name for AddItem To Watch List.
4. Enter the java class name as com.bharosa.vcrypt.tracker.dynamicactions.impl.AddItemToWatchListAction
5. In the Description field, enter a description for the action.
6. In the Notes field, enter any notes you want.
7. Click Load Parameters.
8. For the "Item Type" parameter, enter any one of the following:
   - vtusers - If UserId of current session has to be added to the Watch List
   - devices - If DeviceId of current session has to be added to the Watch List
   - ips - If IP Address of current session has to be added to the Watch List

- countries - If Country Id of current session has to be added to the Watch List
- states - If State Id of current session has to be added to the Watch List
- cities - If City Id of current session has to be added to the Watch List
- userLogin - If LoginId of current session has to be added to the Watch List

9. For the "Watch-List Name" parameter, enter the name of the Watch List. Make sure there is a group with the same name.
10. For the "White-List Name" parameter, enter the name of the White List. Make sure there is a group with the same name. Action will check this list before adding an item to Watch List.
11. For the "Black-List Name" parameter, enter the name of the Watch List. Make sure there is a group with the same name. Action will check this list before adding an item to Watch List

6

Creating Runtimes

A Runtime is a specified point in a session when Adaptive Access Manager collects and evaluates security data using the rules engine.

New Runtimes can be added and existing Runtime properties can be modified using Enumerations Editor Interface.

This chapter describes how to create and configure a new Runtime and how to modify an existing Runtime.

6.1 Creating a New Runtime

To create a new Runtime, follow the instructions below.

1. Log in to Adaptive Risk Manager as a system administrator.
2. On the Environment menu, click Enumerations.
3. Enter "profile.type.enum" in the Enumeration field to search for the available Runtimes.

   The available Runtimes are shown in the Element box.
4. Click the Add New button located under the Element box.

   An Add Element box appears.
5. Enter a value for the Runtime ID.

   The ID value must be a unique identifier for the Runtime. For example, "cancelOrder."
6. Enter a value for the Runtime.

   The value must unique number. Make sure no other Runtime uses the identifier. This ID is like a primary key in database terminology. For example, "1001."
7. Enter a name for the Runtime.

   The name must be user-presentable and meaningful. The name will be used in Adaptive Risk Manager Online. For example, "Cancel Order."
8. Enter a description for the Runtime.
9. Click Create.
10. If the Runtime creation is successful, add the appropriate properties by clicking the Add New button under the Properties box.

    The required properties are:

    - finalactionrule=process_results.rule

The "finalactionrule" property specifies the Rule file that decides the final action. When the Rules Engine processes the policies for the Runtime, it determines the score and a list of actions. The rule file is consulted to see what action should be given as final action. If you are not sure, set the value as in the other Runtimes.The out-of-the-box "process_results.rule" file is sufficient for most actions.

- listTypes= vtusers

  Always set listTypes to "vtusers."

  The models can be linked to only usergroups.

- ruleTypes= user,device,location,in_session

  The "ruleTypes" property defines the list of rule types supported during the Runtime. Depending on the context of the Runtime, possible values are "user," "device," "location," and "in_session." Use commas to separate multiple values. All Rules of the comma separated types can be used in this Runtime.

  For example if ruleTypes is set to "user,location," the Rules of the type "user" and "location" can be used in this Runtime, and the user and location information will be available for this Runtime.

  Another example, for the "Cancel Order" Runtime, if "user,device,location" are specified for ruleTypes, the "user" Rule type expects that the user information will be available during the "Cancel Order" Runtime. If the user information is not available at the time of the "Cancel Order" Runtime, "user" should not be included in the list.

Other properties you may add are:

- isPreAuth

  True indicates that this Runtime is a pre-authentication Runtime. Adaptive Risk Manager will update the user details with the pre-auth score and pre-auth action. The default for isPreAuth is "false." Note that there cannot be two Runtimes with this flag set to "true." Also the same Runtime cannot be marked as postAuth and preAuth.

- isPostAuth

  True indicates that this Runtime is a post-authentication Runtime. Adaptive Risk Manager will update the user details with the post-auth score and post-auth action. The default for isPostAuth is "false." Note that there cannot be two Runtimes with this flag set to "true." Also the same Runtime cannot be marked as postAuth and preAuth.

11. Restart the server.

6.2 Modifying Properties of a Runtime

To modify properties of a Runtime, follow the instructions below:

1. Log in to Adaptive Risk Manager as a system administrator.
2. On the Environment menu, click Enumerations.
3. Enter "profile.type.enum" in the Enumeration field to search for the available Runtimes.

   The available Runtimes are shown in the Element box.

4. Choose the Runtime you want to edit from the Element box.

5. Choose the Property you want to edit from the Properties box.
6. Change the value in the Property Details box.
7. Restart the server.

6.3 Creating a Runtime Example

The procedure for creating the "addressChange" Runtime is provided below.

1. Log in to Adaptive Risk Manager as a system administrator.
2. On the Environment menu, click Enumerations.
3. Enter "profile.type.enum" in the Enumeration field to search for the available Runtimes.

   The available Runtimes are shown in the Element box.
4. Click the Add New button located under the Element box.

   An Add Element box appears.
5. Enter "addressChange" for the Runtime ID.
6. Enter "88" for the Runtime value.
7. Enter "Address Change" for the Runtime name.
8. Enter "Address Change Runtime" for the Runtime description.
9. Click Create.
10. Select "profile.type.enum.addressChange" in the Element box.
11. For finalactionrule, enter "process_results.rule" and click Save.

    The Final Action for a given Runtime during rules evaluation is determined by this rule file. File process_results.rule is supplied out-of-the-box and no additional steps are required.
12. For isPreAuth, enter "true" and click Save.
13. For listType, enter "vtusers" and click Save.
14. For ruleType, "enter user,device,location" and click Save.
15. Restart the server.

The enumeration for the Address Change Runtime is shown below for your reference.

```
profile.type.enum.addressChange=88
profile.type.enum.addressChange.name=Address Change
profile.type.enum.addressChange.description=Address Change Runtime
profile.type.enum.addressChange.ruleTypes=user,device,location
profile.type.enum.addressChange.listTypes=vtusers
profile.type.enum.addressChange.finalactionrule=process_results.rule
profile.type.enum.addressChange.isPreAuth=true
```

7

Transaction Definitions

A Transaction is any process a user performs after successfully logging in. Examples of Transactions are making a purchase, bill pay, money transfer, stock trade, address change, and others.

With each type of Transaction, different type of details are involved. For example, in a stock trade, the data involved would be the symbol, unit price, number of shares, buy or sell action, time of trade, total amount, broker commission, and so on.

Before the client-specific Transaction with its corresponding Entities can be captured and used for enforcing authorization rules, fraud analysis, and so on, it will need to be defined to the system first. Adaptive Risk Manager's Transaction Detail feature allows administrators to perform this task.

With Adaptive Risk Manager's Transaction Definition feature, an administrator is able to create entity and data element definitions and map them to the client-specific data (source data).

This chapter focuses on the creation of Entities and Transaction Definitions. Information on other procedures will also be provided.

7.1 Prerequisites for Using Transactions

The prerequisites for using Transactions is as follows:

1. Using the Transactions feature involves native integration.
2. Transaction data is saved into Adaptive Risk Manager using the APIs described in the *Oracle Adaptive Access Manager Developer's Guide*.
3. An Entity is a set of fields. It is like a user-defined structure that can be re-used across different transactions. Only appropriate and related fields should be grouped into an Entity.

7.2 Configuring a Transaction Definition Overview

Configuration of a Transaction Definition involves the following tasks:

1. Identify all the Entities related to the third-party Transaction.

   Typical Entities are Address, Account, CreditCard, Customer, ProductDetails, and others.

2. Use the Entity Definition user interface to create Entity Definitions.

   Refer to the "Creating an Entity" section.

3. Activate the Entity Definition using the Activate button in the Entity Definition user interface.
4. Create the Transaction Definition using the Transaction Definition user interface.

   Refer to the "Creating the Transaction Definition" section.
5. Add the Entities to the Transaction Definition using the Entities tab in the Transaction Definition user interface.

   Refer to the "Adding Entities to the Transaction Definition" section.
6. Add Transaction data elements using the Data tab in the Transaction Definition user interface.

   For example, TransactionAmount and TransactionDate.

   All data fields that do not fit into entities should be added as transaction data elements.

   Refer to the "Adding the elements that need to be added directly to the Transaction Definition" section.
7. Add the source data elements to the Transaction Definition using the Source Data tab in the Transaction Definition user interface.

   Source data elements are the list of fields that are coming from the external application. Make sure the source data "keys" match the "keys" used by the external application while sending the transaction data.

   Refer to the "Adding the source data elements to the Transaction Definition" section.
8. Add the mapping for the data elements using the Data Mapping tab.

   Refer to the "Adding the mapping for the data elements" section.
9. Add the mapping for the Entity elements using the Entity Mapping tab.

   Refer to the "Adding the mapping for the Entity elements" section.
10. Activate the Transaction Definition.

7.3 Creating an Entity

7.3.1 Initial Steps

To create an Entity, follow the steps below.

1. From the Admin menu, select Entities.
2. For the Entity Name field, choose Create New Entity.
3. Enter the Entity name.
4. Enter the Entity ID.

   The Entity ID is a string that will indicate the Entity.
5. Enter a description.
6. Click Save.

7.3.2 Specifying what elements are part of the Entity

In the Data tab, you will specify what elements are part of that Entity. For example, for an Entity like Address, the elements will be AddressLine1, AddressLine2, City, State, Country, and ZipCode.

1. Select Ext ID if there is an Ext ID value.

   The client supplies the Ext ID value. Oracle Adaptive Risk Manager can either store this value for the client or use it to identify the Entity. For example, a client may send merchant, product, and customer Entities. These Entities will already have IDs with the client.

2. Provide a label.

3. Provide an Int ID.

   The Int ID is used to identify a data element in the Entity. The keys specified in the Data tab will be for internal use. They are typically used in rule conditions and other purposes. Do not change this key after it is defined.

4. Provide a description.

5. Specify whether the element is required.

   Some data elements are not populated all the time as the data might not be available. Those elements are marked as "not required." For example "Address Line 2" in an address is not required since many addresses will not have "Address Line2."

6. Specify whether the element should be encrypted.

   If encrypted is set to true, data is encrypted before it is stored in the database. This feature protects sensitive data.

   Encrypted fields have the following constraints:

   - These fields cannot be used in rules.
   - These fields cannot be used in the search criteria while querying for transactions through the query screen

7. Specify its data type.

8. If you want to add another element, click Add Row and repeat steps 1 through 7.

9. Click Save.

7.3.3 Selecting the elements that can be used to uniquely identify the Entity

In the ID Scheme tab, you will select the elements that can be used to uniquely identify an Entity.

To select the elements, follow the steps below.

1. Select the Data Identification Scheme tab.

   The scheme determines whether the elements that are selected should be stored as plain text (key) or encrypted (digest). The digest scheme is used when the data field value is too large or when there is sensitive data.

2. Add the elements to the ID Scheme.

3. Select the order of the elements

   The order determines how the data is concatenated while forming the data that identifies the Entity. If you don't enter an order, it will be created automatically.

7.3.4 Selecting the data elements that form the Entity data that can be displayed

In the Display tab, you will select the data elements that form the Entity data that can be displayed.

To select the data elements, follow the steps below.

1. Select the Display tab.
2. Select the data elements you want to display by clicking Add.
3. Select the order of the elements

   The order determines how the data is concatenated while forming the data to be displayed for the Entity.

7.3.5 Activating the Entity definition

Activate the Entity definition using the Activate button.

7.4 Creating the Transaction Definition

7.4.1 Initial Steps

To create a Transaction Definition, follow the steps below.

1. On the Admin menu, select Transactions.
2. For the Transaction Definition Name field, choose New Transaction Detail.
3. Enter the Transaction Definition name.
4. Enter the value for the transaction key.

   This key value is used to map the client/external transaction data to transactions in Adaptive Risk Manager.

   This value should be sent as the TransactionKey while making the API call for creating or updating the transaction data in Adaptive Risk Manager.
5. Enter the description.
6. Click Save.

7.4.2 Adding Entities to the Transaction Definition

The Entities tab is chosen by default after clicking Save during Transaction Definition creation in the previous section.

To add Entities to the Transaction Definition, follow the steps below.

1. Pick an Entity from the Entity Name menu.

   The Entities available are the ones we defined earlier in the "Creating an Entity" section.
2. Enter the instance name.
3. Enter the relationship type.

   For example, Address can be a Billing Address or a Shipping Address.
4. Enter the display order.

5. Click Save.

7.4.3 Adding the elements that need to be added directly to the Transaction Definition

Elements are defined internally. To add elements that need to be added directly to the Transaction Definition, follow the steps below.

1. Select the Data tab.
2. Click Add Row.
3. Enter the data name.
4. Enter the data type.
5. Enter the key.

   The key is used to identify the data element. The keys specified in the Data tab will be for internal use. They are typically used in rule conditions and other purposes. Do not change this key after it is defined.
6. Enter a description.
7. Specify the row and column.

   If there is a need to change the Row and Column values, please follow the guidelines below:

   a. Set the column values for the most commonly used fields to 1-3 or 11-13 based on whether it is non-numeric or numeric.
   b. For a given row there can be a total of 13 fields.
   c. For Non-Numeric fields, Column value should be 1 to 10.
   d. For Numeric fields, Column value should be 11 to 13.

   Fields in the Data tab are mapped to DATAX (for non-numeric), NUM_DATAX (for numeric) columns in VT_TRX_DATA table in database.

   Fields in Entities are mapped to DATAX (for non-numeric), NUM_DATAX (for numeric) columns in VT_ENTITY_ONE_PROFILE table in database.
8. Specify whether the element should be encrypted.

   If encrypted is set to true, data is encrypted before it is stored in the database. This feature protects sensitive data.

   Encrypted fields have the following constraints:

   - These fields cannot be used in rules.
   - These fields cannot be used in the search criteria while querying for transactions through the query screen
9. Specify whether the element is required.

   Some data elements are not populated all the time as the data might not be available. Those elements are marked as "not required." For example "Address Line 2" in an address is not required since many addresses will not have "Address Line2."
10. Add other elements by following steps 2 through 9.
11. Click Save.

7.4.4 Adding the source data elements to the Transaction Definition

The source data is defined by the client. To add source data elements to the Transaction Definition, follow the steps below.

1. Select the Data Source tab.
2. Click Add Row.
3. Enter the data name.

   The data name provides a way to identify the element; especially if the key is cryptic. For example, the data name could be Transaction.amount while the key could be D1212.
4. Enter the data type.
5. Enter the key.

   The client supplies the key.
6. Enter a description.
7. Specify whether the source data is needed.
8. Add other elements by following steps 2 through 7.
9. Click Save.

7.4.5 Adding the mapping for the data elements

Mapping is a way to connect the source data to our Entities/data.

To add the mapping for the data elements, follow the steps below.

1. Select the Data Mapping tab.
2. Choose the destination data.

   The data elements to choose from are the ones you defined in the "Adding the elements that need to be added directly to the Transaction Definition" section.
3. Pick the mapping type.

   Select Direct, Concatenate, Endstring, and Substring.

   - Choose Direct if you want a one-to-one mapping of the source data element to the destination data element.
   - Choose Concatenate if you want to join two or more source data elements to form one data element.
   - Choose Endstring if you want to have last "x" number of characters from source data as the data.
   - Choose Substring if you want to have a part of the source data as the data.
4. If you selected Concatenate as the mapping type, you will have to enter separators.
5. If you selected Endstring, you will have to enter the last "x" number of characters.

   If you selected Substring, you will have to enter the Start Index and the End Index (CSV format). For example if you want "acc" for "account," you would specify 1,3.

   Translation Params are the parameters defined when selecting certain Mapping type such as endstring, lowerstring, and substring.
6. Pick the Source Data.

The client data elements to choose from are the ones that you added in the "Adding the source data elements to the Transaction Definition" section.

7. Map other elements by following steps 2 through 6.
8. Click Save.

7.4.6 Adding the mapping for the Entity elements

To add the mapping for the Entity elements, follow the steps below.

1. Select the Entity Mapping tab.
2. Pick the Entity.
3. Select the destination data.
4. Pick the mapping type.

   Select Direct, Concatenate, Endstring, and Substring.

   - Choose Direct if you want a one-to-one mapping of the source data element to the destination data element.
   - Choose Concatenate if you want to join two or more source data elements to form one data element.
   - Choose Endstring if you want to have last "x" number of characters from source data as the data.
   - Choose Substring if you want to have a part of the source data as the data.
5. If you selected Concatenate as the mapping type, you will have to enter separators.
6. If you selected Endstring, you will have to enter the last "x" number of characters.

   If you selected Substring, you will have to enter the Start Index and the End Index (CSV format). For example if you want "acc" for "account," you would specify 1,3.

   Translation Params are the parameters defined when selecting certain Mapping type such as endstring, lowerstring, and substring.
7. Select Source Data.
8. Click Save.

7.4.7 Activating the Transaction Definition

Activate the Transaction Definition using the Activate button.

Some steps are required before a transaction definition can be activated; otherwise, an error message will appear.

The following are required before you can activate a transaction definition:

- Source/Input data elements
- Mapping for all required Transaction Data Elements
- Mapping for all required elements in the Transaction Entities

7.5 Listing Entities

To list Entities

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Entities, and then click List Entities.
3. Select the criteria you want to filter the Entities on.
4. Click the Run Query button.

7.6 Listing Transactions

To list Transactions

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Transactions, and then click List Transactions.
3. Select the criteria you want to filter the Transactions on.
4. Click the Run Query button.

7.7 Exporting Entities

To export Entities

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Entities, and then click Export Entities.
3. Select the criteria you want to filter the Entities on.
4. Click the Run Query button.
5. Select the Entity you want to export.
6. Click the Export button.
7. Click OK.
8. Click Save To Disk and then click OK.

7.8 Exporting Transactions

To export Transactions

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Transactions, and then click Export Transactions.
3. Select the criteria you want to filter the Transactions on.
4. Click the Run Query button.
5. Select the Transaction you want to export.
6. Click the Export button.
7. Click OK.
8. Click Save To Disk and then click OK.

7.9 Importing Entities

To import Entities

1. Log in to Adaptive Risk Manager.

2. On the Admin menu, point to Entities, and then click Import Entities.
3. Browse for your Entities zip file.
4. Click the Import button.

7.10 Importing Transactions

To import Transactions

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Transactions, and then click Import Transactions.
3. Browse for your Transactions zip file.
4. Click the Import button.

7.11 Modifying Entities

To modify Entities

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Entities, and then click Create Entities.
3. Select the Entity you want to modify from the Entity Name list.
4. From the top portion of the screen, you can modify the name, Entity ID, and description of the Entity; and activate or deactivate the Entity.
5. From the bottom portion of the screen, you can modify the data elements of the Entity.

Note: When modifying Entities, do not change the key. The key may be referenced by other applications.

7.12 Modifying Transactions

To modify Transactions

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Transactions, and then click Create Transactions.
3. Select the Transaction Definition you want to modify from the Transaction Definition Name list.
4. From the top portion of the screen, you can edit the name and description of the Transaction Definition; and activate or deactivate the Transaction Definition.
5. From the bottom portion of the screen, you can edit the Entity and data elements of the Transaction.

Note: When modifying Transactions, do not change the key. The key may be referenced by other applications.

7.13 Viewing the Transaction Data in Adaptive Risk Manager

After the Transaction Definition is created, Adaptive Risk Manager will be able to capture information when the client application sends the data.

To view the data the client application sends:

1. On the Queries menu, select User, Location, or Device.
2. Select the criteria you want to filter on.
3. Click the Run Query button.
4. On the Recent Logins page, click the Session link.
5. On the Session Details page, click the Transaction Details link.

8

Auto-learning and Patterns

Auto-learning is a profiling process in which an administrator defines behavior patterns. These patterns are in turn used by Adaptive Risk Manager to dynamically create and populate buckets based on the pattern parameters.

Adaptive Risk Manager automatically records/maintains the bucket memberships of the users/devices/locations (entities in general) over time so that the profiles created can be used to evaluate risk. Entities—users, devices, and locations—are pattern members, and sometimes referred to as actors.

This chapter will focus on creating and using patterns. Information will also be provided on listing, importing, exporting, and activating and deactivating patterns.

For conceptual information on Auto-learning and patterns, refer to *Oracle Adaptive Access Manager Concepts*.

8.1 Introduction and Concepts

This section introduces you to the concept of patterns and how they are used in Adaptive Risk Manager.

8.1.1 About Patterns

Patterns are a composite of traits or features characteristic of an individual or a group. Patterns are created as buckets (groupings of behaviors) by Adaptive Risk Manager.

Adaptive Risk Manager collects data and populates these buckets with members based on pattern parameters. Auto-learning, a feature of Oracle Adaptive Access Manager, profiles transactions and authentications being performed by different actors (entities).

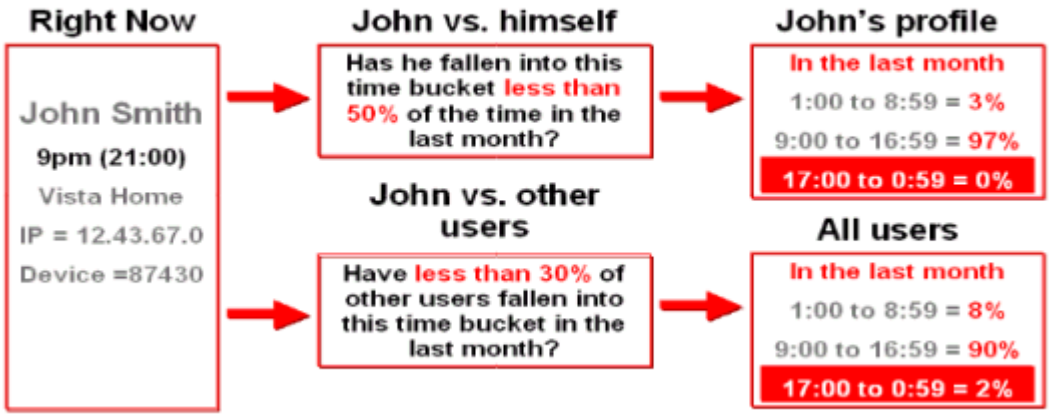
For example, if we want to find out the typical log in times (time of day) for users, we would set up a pattern. The pattern would be set up so that the user is a member and time is a parameter.

We would choose to create a multi-bucket pattern and set start time=00 and endtime=23 (these are hours of the day). We choose to create a multi-bucket pattern since it will create multiple range buckets rather than a single-bucket pattern, which has single data points and value ranges.

When users log in, profiles will automatically be created for each user at log in time. When Adaptive Risk Manager gathers this data for a few days or months, Adaptive Risk Manager can use this data to challenge the user if he logs in at a time at which he does not usually log in.

8.1.2 About Auto-learning

The Auto-learning feature profiles transactions and authentications being performed by different actors (entities). This process establishes what is normal or average behavior for an individual or a population.



In turn this allows evaluations to be made that can determine if a situation is an anomaly and therefore potentially fraudulent.

The task is accomplished by

- capturing the transaction and authentication data and passing it through various patterns thereby creating/populating various buckets to profile behavior in a granular way.
- capturing the behavioral and transaction data, based on the actors (entities), and then creating the statistics for the entities based on their memberships to various patterns and hour/day/month/year time samples.

8.1.3 About Buckets

Patterns are created as single-buckets or multi-buckets. Buckets are groupings of behaviors that enables Auto-learning to profile behavior in a granular way.

- Single-Bucket

  Single-bucket patterns will create and populate one bucket with the exact data points and value ranges specified in the pattern.

  For example, if you choose to create an authentication pattern for users (member type) with the country United States (attribute), exactly one bucket will be created and populated with users. If a user logs in from the United States, he becomes a member of the bucket and his counts are incremented; if he does not log in from the Untied States, his member count is not incremented for this bucket.

- Multi-Bucket

  Multi-bucket patterns have buckets for sub-ranges of a parameter range. For example, if you choose user logins for a 24-hour range with a step size of 8, there will be 3 buckets for 8-hour time slots in which logins can occur.

8.2 Before You Begin

To use the Auto-learning feature, you must perform the following procedures.

8.2.1 Import Default Entities

You must import default entities into your system. Auto-learning data collection and rules will not run properly without them. Default entities are shipped along with Oracle Adaptive Access Manager in the Auth_EntityDefinition.zip file in oaam_init.

To import the entities:

1. On the Admin menu, point to Entities, then click Import Entities.
2. Click Browse and locate Auth_EntityDefinition.zip.
3. Click Import.

   Adaptive Risk Manager will show the entities in that file.
4. Select and import all of them.

8.2.2 Enable Auto-learning properties

Enable Auto-learning so that Adaptive Risk Manager Online/Offline collects data.

1. Ensure that vcrypt.tracker.autolearning.enabled is set to true.

   This property must always be set to true. It is like a "master (on/off) switch" for Auto-learning.
2. Using the Properties Editor, set the following properties to true:
   - vcrypt.tracker.autolearning.use.auth.status.for.analysis

     This property must be set to true for the auth patterns to work.
   - vcrypt.tracker.autolearning.use.tran.status.for.analysis

     This property must be set to true for all transaction patterns to work.
3. If the properties are needed and do not exist, create them using the Properties Editor.

8.2.3 Configure Patterns

Auto-learning patterns need to be defined and enabled.

8.2.4 Use API for updateStatus

Before auto-learning can perform monitoring of transactions and authentications, patterns must be configured and clients must use the correct API for updateStatus. For more information on Auto-learning APIs, refer to "Auto-learning" in the *Oracle Adaptive Access Manager Developer's Guide*.

8.3 Using Patterns in Adaptive Risk Manager (Overview)

Pattern-based Rule Template and related conditions are available out-of-the-box.

For a pattern to be used in Adaptive Risk Manager, you would

1. Determine what you want Adaptive Risk Manager to watch for (as a potential fraud behavior).

2. Create the pattern using the Create Patterns user interface.

   Refer to the "Creating a Pattern" section.

3. Configure a Rule Template for patterns (or pick an existing one).

   This chapter will provide an example for creating a Rule Template for patterns. Refer to the "Creating a Rule Template for Patterns" section.

4. Create a Model (or pick an existing Model) that uses patterns.

   a. Pick the Rule Template from step 3.

   b. Select the pattern you want the Rule to act upon.

   This chapter will provide an example for creating a Model that uses patterns. Refer to the "Creating a Model that Uses Patterns" section.

8.4 Creating a Pattern

To create a pattern

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Patterns, and then click Create Patterns.
3. Choose a Transaction Type.

   The transaction types shown will be whatever Transaction Definitions have been configured in the specific Adaptive Risk Manager installation. Examples of Transaction Types are authentication, bill pay, money transfer, merchant purchase, credit card, and others. For example, if you pick merchant purchase as the Transaction Type, you want to gather data on the activity of all the members during merchant purchases.

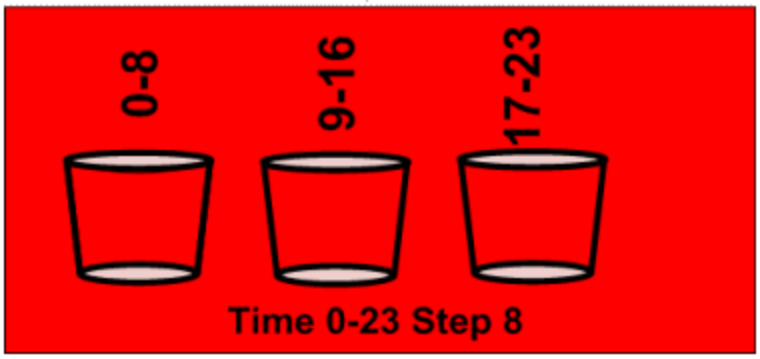
4. From the Creation Method list, choose which method you want to use to create the pattern.

   - Single-Bucket

     Single-bucket patterns will create and populate one bucket with the exact data points and value ranges specified in the pattern.

   - Multi-Bucket

     Multi-bucket patterns have more data points. Multi-bucket patterns will create and populate buckets for sub-ranges of a parameter range.



5. For Pattern Name, select Create New Pattern.
6. Type in the pattern name.

   The pattern name must be unique.
7. Choose Status
   - Active

     If data needs to be collected, the pattern must be in the active state.
   - Inactive

     If the pattern is complete, but you don't want to collect data, pick "Inactive."
   - Incomplete

     If pattern creation has started, but you need to save it for completion later, choose "Incomplete." Data is not collected for this state.
   - Invalid

     The administrator may choose to mark the pattern as invalid if he does not want the pattern used. Data is not collected for this state.
8. Choose Member Type.

   The member type is the actor for which data needs to be captured.
9. Choose a Evaluation Priority
   - First

     The data is evaluated in realtime (highest priority)
   - Second

     The data is evaluated in near-realtime (low priority). If the server has a large system load, the patterns marked as "second" can be skipped. The system load is the number of authentication, transaction, rule processing (and other) reports and requests served by the Oracle Adaptive Access Manager server.
10. Enter a description.
11. Click Save

    If you try to create a pattern with the same entities as another pattern, a message will appear: "A pattern with the same entity configuration already exists. Are you sure you want to create a new pattern? If you answer "yes," you will be allowed to create the pattern.
12. Add Attributes

Pick attributes related to the member type. Adaptive Risk Manager will collect data on the attributes to be used in the pattern membership.

For example, if you pick "user" as the member type and the attributes: IP (NNN.N.N.N), City (Redwood City) and Is Registered (False); Adaptive Risk Manager will record when users match all of these attributes. This profiling can then be used to evaluate risk for the "user."

The following attributes are available:

- ASN: A unique identifier of an autonomous system on the Internet. Along with other comparators, "for each" is available because if you come from another ASN, you could track that as another bucket. For this attribute, the "equal to" comparator is not available because users will not know the ASN since it is not exposed.
- City
- Country
- Device Id
- Group Id
- IP: This is the IP address where the authentication is coming in from. It could be the real IP of the user, anonymizer, proxy, or gateway, and so on, to which the end user is connected to.
- ISP: The ID for an Internet connection service provider.
- Is Registered: This attribute tracks if the user needs to be tracked on the "isRegistered" criterion. So if the user is a registered user (completed registration), he is treated in the pattern one way, and if he is not a registered user (has not completed registration), he is treated another way.
- Login Id: User Id
- State
- Time
- Username

13. Enter the Status.
    - Active

      Data is collected on the attribute. For example, if you have 5 attributes and you want data collected on all of them, all 5 attributes would be in the active state.
    - Inactive

      Data is not collected on the attribute. For example, if you have 5 attributes and you only want to collect data for 2 of them. You would mark the 3 you don't want to collect data on as inactive.
14. Enter a description.
15. Enter an order.
16. Select a compare operator.

    The list of compare operators depends on the value of the attribute and the type of pattern (multi-bucket or single bucket) you have chosen.
17. Enter a value to compare the incoming data with.

For the operators, "Like" and "Not Like," data can be separated with commas.

8.5 Creating a Rule Template for Patterns

To be able to use a pattern, you can create a Rule Template with conditions for patterns.

Refer to the Rule Template for detail information on creating a Rule Template and modifying Rule conditions.

1. Create a Rule with at least one condition for patterns.

   For example, you could create a Rule Template with the condition, USER: User is member of pattern N times.

   Other Rule conditions for patterns are also available out-of-the-box.

2. During Rule creation, you can customize conditions if you want.

   Parameters for the USER: User is member of pattern N times condition is shown below as an example.

Label	Name	Default
Pattern Hit Count More than	patternHitCountForUser	0
Pattern Name	patternNameForUser	
Time period for pattern membership	timePeriod	1
Time period type for pattern membership	timePeriodType	time.unit.enum.hour
Is Membership Count More than patternHitCountForUser	isMoreThan	true

   Labels are the names the client will see in the condition section when he is adding a Rule to a Model. For example, you can change "Pattern Hit Count More than" to "Behavior Count More than."

   Names are for internal use to identify the parameter if the label has been changed. Names can also be changed.

   Defaults are ones that will be used for the condition if the user does not change them when adding the Rule to a Model. If the defaults are changed, the new values will be seen in the condition section when the user is adding a Rule to a Model.

   As an example, the parameter descriptions for the "USER: User is member of pattern N times" condition are provided below:

   - Pattern Hit Count More than: The number you want to compare your data against. If Pattern appears more than "x" number of times, trigger the Rule.
   - Pattern Name: The pattern you want to use to profile all specified member types.
   - Time period for pattern membership: The numeric value to be used in specifying the time range to check the data against for pattern membership. For example, "3" in 3 months.
   - Time period type for pattern membership: The unit to be used in specifying the time range to check the data against for pattern membership. For example, "months" in 3 months.

- Is Membership Count More than patternHitCountForUser: For most cases, if this parameter is set to true, the rule (that the condition belongs to) will trigger if the condition is true. For example, if the condition is for a user to log in from a certain city and you set the pattern hit count as more than 30. If you set the parameter to true, if the condition is met and the hit count has been more than 30, the rule will be triggered. Another example, suppose a user doesn't log in. If the condition is for a user to log in and you set the pattern hit count to be 0. If you set the parameter to false, if the condition is not met and the hit count is 0, the rule will trigger.

3. When you create the rule template with the conditions, you will have to specify the order in which the condition will be used to check data against.

   For example, you may have more than one condition.

   The order check box is found in the Create Rule Template page.

8.6 Creating a Model that Uses Patterns

For detail information on creating a Model, refer to Chapter 3, "Rules and Models."

To create a Model that uses patterns, you would

1. Pick a Rule that is used specifically for patterns. For example, a Rule that has the condition, USER: User is member of pattern N times.
2. Select the pattern you want the Rule to act upon. For example, in the "USER: User is member of pattern N times" section in the Add Rule box, select your pattern from the Pattern Name list.
3. If you do not like the defaults given in the Conditions section, change them.

   As an example, the parameter descriptions for the "USER: User is member of pattern N times" condition are provided in the "Creating a Rule Template for Patterns" section.

8.7 Listing Patterns

To list patterns

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Patterns, and then click List Patterns.
3. Select the criteria you want to filter the patterns on.
4. Click the Run Query button.

8.8 Exporting Patterns

To export patterns

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Patterns, and then click Export Patterns.
3. Select the criteria you want to filter the patterns on.
4. Click the Run Query button.
5. Select the pattern you want to export.
6. Click the Export button.

7. Click OK.
8. Click Save To Disk and then click OK.

8.9 Importing Patterns

To import patterns

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Patterns, and then click Import Patterns.
3. Browse for your patterns zip file.
4. Click the Import button.

8.10 Deactivating/Activating Patterns

To deactivate or activate patterns

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Patterns, and then click List Patterns.
3. Select the criteria you want to filter the patterns on.
4. Click the Run Query button.
5. Select the pattern you want to deactivate or activate.
6. Press the Inactive or the Active button.

When Patterns are disabled, the data collection stops.

Also when rules are executed and the pattern being used by the rule condition is not active, the condition evaluates to false (unless you have configured it to return true).

You should be extremely careful when disabling patterns. The system does not check if the pattern being disabled is used in any model.

8.11 Deleting Patterns

To delete a pattern

1. Log in to Adaptive Risk Manager.
2. On the Admin menu, point to Patterns, and then click List Patterns.
3. Select the criteria you want to filter the patterns on.
4. Click the Run Query button.
5. Select the pattern you want to deactivate or activate.
6. Press the Delete button.

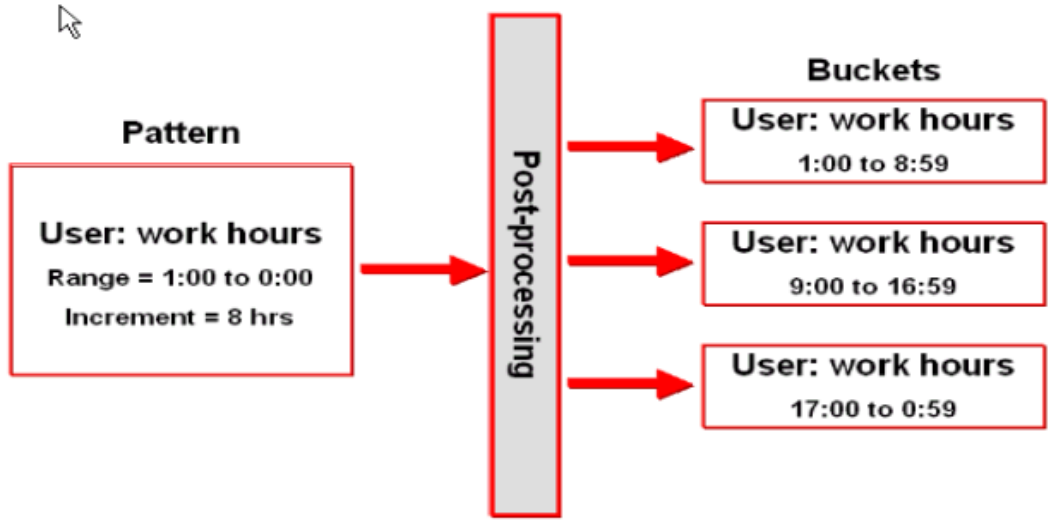
Patterns can be deleted only if there is no association with data and rules. If you have an active pattern and it has collected data, you will not be able to delete the pattern.

The following message appears:

There might be pattern data or associated rules using the data and may become out of sync. Are you sure you want to update?

8.12 Pattern Scenario

An administrator creates a pattern for behavior-based profiling on time. Adaptive Risk Manager creates buckets through post processing for the behavior.



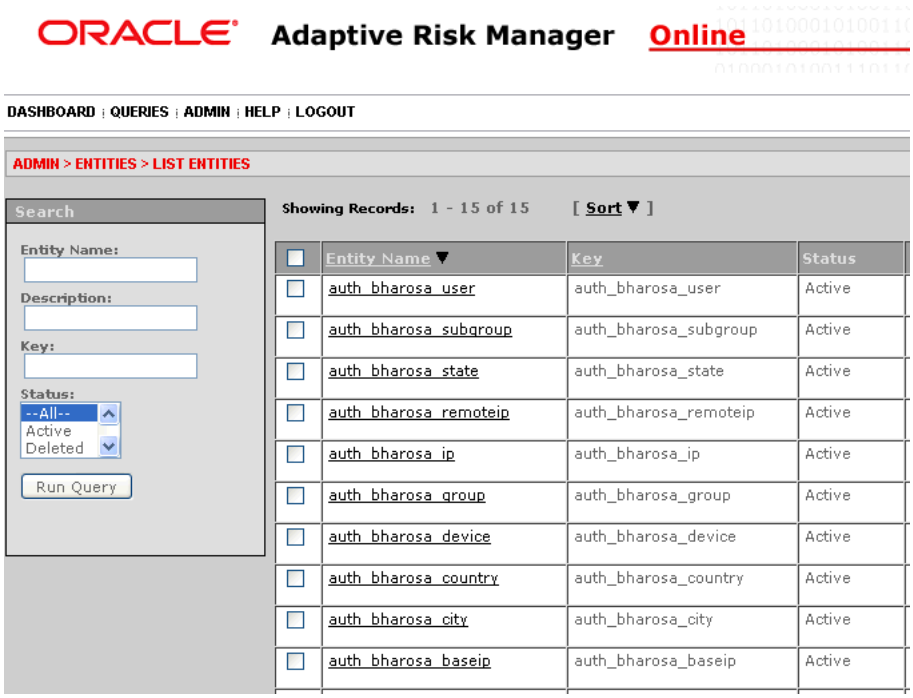
8.13 Troubleshooting

To find out if Auto-learning pattern analysis is working, follow the steps below:

8.13.1 Ensure Default Entities are Set Up

Make sure you have the default entities set up.

On the Admin menu, point to Entities, then click List Entities. You must see entities like the ones shown below.



If you are not seeing these entities, you will need to import them.

The Auth_Entities.zip file is shipped along with the Oracle Adaptive Access Manager binaries. Locate that file and import it as entities using the Admin->Entities->Import Entities menu.

8.13.2 Ensure properties settings are correct

Make sure the Auto-learning properties are set correctly on your system as described below.

Of particular importance are the following properties:

Property	Default Value	Property Type	Is Dynamic	Comments
vcrypt.tracker.autolearning.enabled	true	Boolean	Yes	Make sure this is set to true.

Property	Default Value	Property Type	Is Dynamic	Comments
vcrypt.tracker.autolearning.use.auth.status.for.analysis	false	Boolean	Yes	Make sure this is set to true. This flag is used where client code does not explicitly call the Auto-learning API. So if you want Auto-learning (post processing) to take place but do not want to change the client code; then, setting this flag to true will result in Auto-learning processing for authentication type of updateAuthStatus requests; if the status is success for that auth request. However, if status is not success Auto-learning will not occur anyway. Running Auto-learning rules with this flag set to false will mean that you are running the rules on the data that is stale.

Property	Default Value	Property Type	Is Dynamic	Comments
vcrypt.tracker.autolearning.use.tran.status.for.analysis	false	Boolean	Yes	Make sure this is set to true. This flag is used where client code does not explicitly call Auto- learning API. So if you want Auto-learning (post processing) to take place but do not want to change the client code; then, setting this flag to true will result in Auto-learning processing for updateTransactionStatus requests; if the status is success for that transaction request. However if status is not success, Auto-learning will not occur. Running Auto-learning rules with this flag set to false will mean that you are running the rules on the data that is stale.

Part II

Knowledge-Base Authentication

This part provides information about Knowledge-Base Authentication (KBA), the answer logic algorithms, creating and editing new questions, and using the KBA Validation Editor.

Part II contains the following chapter:

9

KBA Challenge Questions

The chapter provides an overview of the KBA (Knowledge Based Authentication). configuration and Oracle's Answer Logic algorithms. Steps for creating, importing, and exporting questions; using the KBA Validation Editor, and KBA security solutions, are also provided.

Topics covered include:

- Using KBA Challenge Questions
- Answer Logic
- KBA Validation Editor
- Configuring the Registration Logic
- Configuring the Answer Logic
- KBA Security Solution Guidelines and Recommended Requirements
- Questions about Collection and Challenge
- Best Practices for Managing Challenge Questions

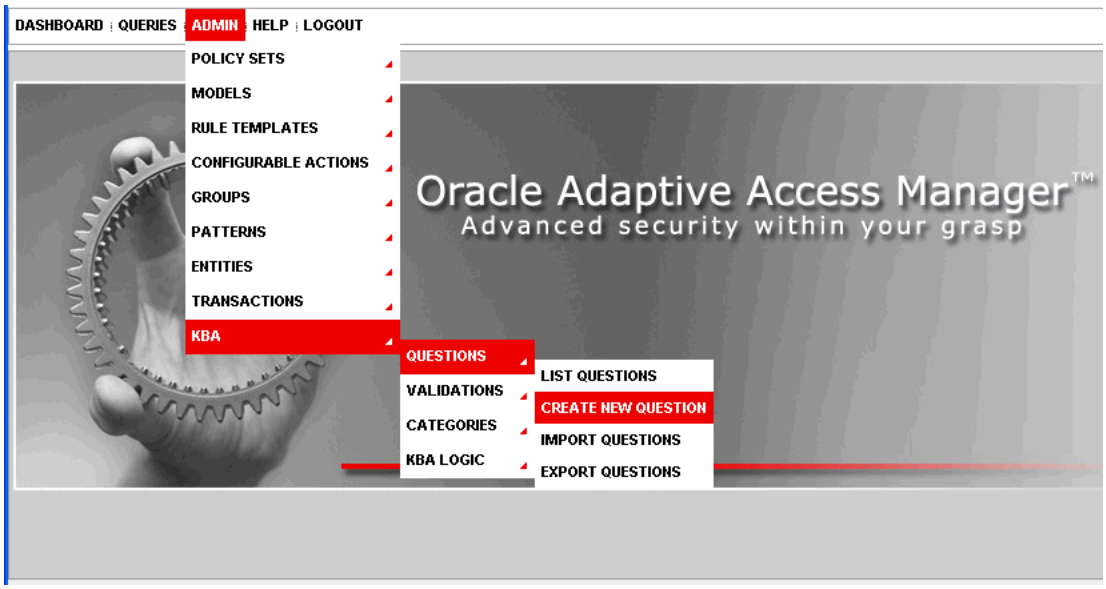
9.1 Using KBA Challenge Questions

The default KBA configuration presents customers with three question menus. When a customer registers, he or she is required to select one question from each menu. These three questions become the customer's "registered questions". The KBA functionality enables you to manage these challenge questions.

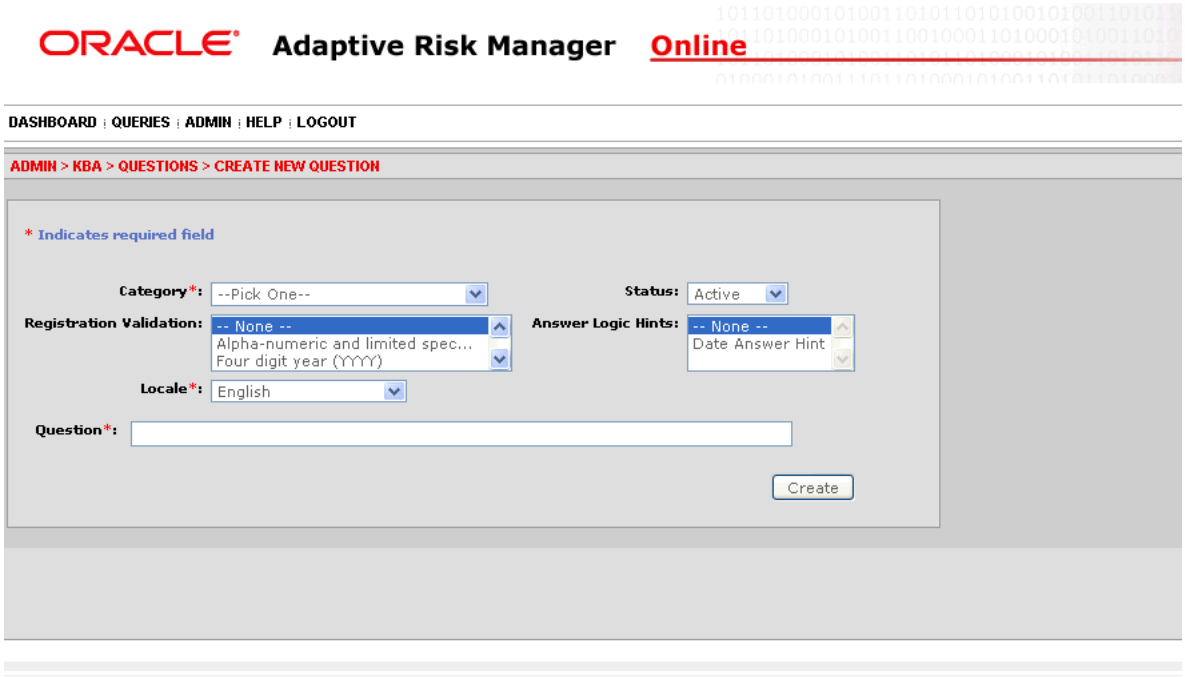
9.1.1 Creating a New Question

To create a new question

1. On the Admin menu, point to KBA, point to Questions, and then click Create New Question.



The Create New Question page appears.



2. Type the new question in the question field.
3. Click in the Category box and select the category of question you want.

   By default, there is no data in the Category menu. You must import the Security Questions zip files (oaam_kba_questions_<locale>.zip) for data to appear in the Category menu. You can also create a new category; data will appear in the Category menu.
4. In the Registration Validation list, click the type of registration validation you want.

5. Click in the Status box and select the status you want.
6. In the Answer Logic Hints list, click the type of Answer Logic Hint you want. These hints help the answer logic function more successfully on some questions, for example, on date related questions.
7. Click in the Locale box and select the language you want.

   By default, the Locale menu displays English and 26 other default locale languages. For additional information on how to enable languages, see "Globalization Support" in the *Oracle Adaptive Access Manager Installation and Configuration Guide*.
8. Click Create.

   The Question Detail page appears for the newly created question.

9.1.2 Editing a Question

You can activate, disable, and edit a question on the Question Details page. If a question is disabled, new registrations will not get this question; customers who have previously selected this question are not affected. If you edit a question, customers using that question will receive the updated question.

To edit a question

1. On the List Questions page, click the wrench icon next the question you want to edit.

   The Question Details page appears.
2. Make the changes you want and click Save.

9.1.3 Viewing a List of All Questions

On the List Questions page you can view a list of all challenge questions and search the question repository based on various criteria. The List Questions page provides access to the Questions Details page for any question.

1. On the Admin menu, point to KBA, point to Questions, and then click List Questions.

   The List Questions page appears.
2. To display only the category of questions you want to view, in the Category list click the category you want and click Submit Query.
3. To display questions by registration validation you want to view, click the Registration Validation type from the list and Submit Query.
4. To display only questions with the type of answer logic hint you want to edit, in the Answer Logic Hint list click the type you want and click Submit Query.
5. To display only questions with the status you want to edit, in the Status list click the status you want and click Submit Query.
6. To find a specific question, in the Question ID box enter the ID of the question and click Submit Query.
7. To find a question by keyword, in the Question Keyword box enter the keyword and click Submit Query.

8. To find a question that was created or modified within a specific timeframe, click the calendar icons and select the From Date and To Date you want and click Submit Query.
9. To edit a question in the list, click the wrench icon to the left of the question you want to edit.
10. To delete, enable, or disable a question, select the check box to the left of the question and click the appropriate button above and below the list of questions.

9.1.4 Viewing Categories of Questions

You can search the question categories in the system based on various criteria.

To view question categories

1. On the Admin menu, point to KBA, point to Categories, and then click List Categories.
2. To display a specific question category, in the Category list, click the category you want and click Submit Query.
3. To display categories with a specific status, in the Status list click the status you want and click Submit Query.
4. To find a specific category, in the Category ID box enter the ID of the category and click Submit Query.
5. To find a category that was created or updated within a specific timeframe, click the calendar icons and select the From Date and To Date you want and click Submit Query.
6. To find all categories regardless of timeframe, select Ignore Dates.
7. To delete, enable, or disable categories, click the check box to the left of categories and select appropriate action button above and below list categories.

   New registrations are not be presented with questions from the disabled category.

9.1.5 Importing Validations

To import validations

1. On the Admin menu, point to KBA, point to Questions, and then click Import Validations.

   The Import Validations page appears.
2. Click Browse and locate the Zip file of validations you want.
3. Click Import.

   The Import Validations page appears with a list of the newly imported validations.

9.1.6 Importing Questions

You can import Zip files of questions into the system. If you import questions that belong to a category not currently in the system, the category will also be imported. If you import a question with the same ID# as an existing question, the existing question will be overwritten.

To import questions

1. On the Admin menu, point to KBA, point to Questions, and then click Import Questions.

   The Import Questions page appears.

2. Click Browse and locate the Zip file of questions you want.

3. Click Import.

   The Import Questions page appears with a list of the newly imported questions.

9.1.7 Exporting Questions

To export questions

1. On the Admin menu, point to KBA, point to Questions, and then click Export Questions.

2. Enter search parameters to find the questions you would like to export.

3. Select the questions you want to export then click Export.

9.1.8 Exporting a Delete Script

To export a delete script

1. On the Admin menu, point to KBA, point to Questions, and then click Export Questions.

2. Enter search parameters to find the questions you think you may want to delete in the future.

3. Select these questions and click Export Delete Script.

   Export Delete Script enables you to export a delete script for the questions you have chosen. Later on, you can import the delete script to delete these questions.

9.2 Answer Logic

Challenge questions are set up by the user during the registration process. They are used for additional authentication during high risk situations. Oracle's Answer Logic is used during the challenge response process.

9.2.1 Type of Answer Logic

An overview of Oracle's answer logic algorithms is presented below. The answer logic algorithms can be enabled or disabled using Oracle's Knowledge Based Authentication Configuration in Adaptive Risk Manager. The intensity or strength of some algorithms can also be configured.

This section also highlights the most common response errors and shows how Oracle's Answer logic algorithms are used for the system to intelligently detect the correct answers in the challenge response process.

The following answer logic algorithms are available for both the online challenge and phone challenge processes:

Abbreviations

Common abbreviations, common nicknames, common acronyms, and date format are handled by this algorithm.

Phonetics

Answers that "sound like" the registered answer, regional spelling differences, and common misspellings are handled by this algorithm.

Keyboard fat fingering

Answers with typos due to the proximity of keys on a standard keyboard are handled by this algorithm.

9.2.2 Examples of Answer Logic Algorithms

This section provides some examples of abbreviations, phonetics, and keyboard fat fingering.

9.2.2.1 Abbreviations

Common abbreviations, common nicknames, common acronyms, and date format are handled by this algorithm.

Common Abbreviations

This algorithm will match the words in the following pairs as equivalent. Oracle has predefined list of word-pairs that cover common abbreviations, common nicknames and common acronyms. The list can be customized by updating properties file bharosa_auth_abbreviation_config.properties.

- Street - St.
- Drive - Dr.
- California - CA

Common Nicknames

Oracle has a predefined list of the most common nicknames that is used in the challenge response process.

- Timothy - Tim
- Matthew - Matt

Date Format

The questions that require date as the answer specify the format in which the user should enter the answer. The format is either YYYY or MMDD, but not both. However, from experience, customers still use other formats during the challenge response process. The abbreviation logic for date format sees the following as the same:

- 0713
- 713
- July 13th
- July 13
- July 13, 1970

9.2.2.2 Phonetics

Answers that "sound like" the registered answer, regional spelling differences, and common misspellings are handled by this algorithm.

The phonetics algorithm is only supported in English.

Common Misspellings

Oracle's Phonetic Answer logic algorithm accounts for misspellings.

- ph - f
- Correct word: elephant - Spelling mistake: elefant

9.2.2.3 Keyboard Fat Fingering

Oracle's Fat Fingering algorithm accounts for typos due to the proximity of keys on a standard keyboard and transposed letters. Answers with typos due to the proximity of keys on a standard keyboard are handled by this algorithm.

The number of fat fingering characters allowed depends on the length of the original word and the level set. The algorithm returns a percentage score associated with the characters that have an exact match. The intensity will determine the minimum score required to match the answer with the registered answer.

The fat fingering algorithm is only supported in English.

Common Typos

- Switching "w" and "e"
- Switching "u" and "i"
- Switching "t" and "r"

Examples of Fat Fingering

- Correct word: signature - Fat finger: signatire

9.3 KBA Validation Editor

KBA validations are executed at the time of question registration. Validations are used to validate the answers given by a user at the time of registration. Validations can be associated with each individual question or at the global level to be applied to all the questions presented to the user.

KBA Validation Editor provides the following functions:

- Create validations based on the available validation schemes in the system
- Edit existing validations
- Import validations
- Export validations
- Delete validations

9.3.1 Adding a New Validation

You can add a new validation to the system when needed.

To add a Validation

1. On the Admin menu point to KBA, point to Questions, and then click Validations.

   The Validation List/Editor page appears.

2. In the Validation Scheme list, click the name of the validation scheme you want to add.

You might, for example, select the validation scheme "Maximum Length". This validation scheme allows the user to create a validation for the maximum allowed length for the answer.

The parameters of the validation appear in the "Validation Parameters" area.

3. In the Name box, enter the name you want for this instance of the validation scheme.

   When you create a validation from available validation schemes in the system, you are adding an instance of validation. You can then customize that instance.

4. In the Allowed Characters box, specify validation parameter.

   For example, validation parameter can be '30' for an instance of "Maximum Length" validation. This validation instance will restrict user to enter answer longer than 30 characters in length.

   See Table 9–1, " Validation Parameters" for a description of validation parameters for each validation scheme.

5. In the Error Message box, specify the error message to be given to user when the answer given by user is not passing the validation condition.

   For example, error message can be "Your answers may not be more than thirty characters long." for an instance of "Maximum Length" validation.

6. Click Add.

   Adaptive Risk Manager Online adds this validation instance to the list of validations in the System.

Table 9–1 Validation Parameters

Validation Scheme/Type	Description for Validation Parameter
Minimum Length	Minimum length (number) for the answer. If length of the answer entered by user is less than the configured value then validation will fail and user will get configured error message.
Maximum Length	Maximum allowed length (number) for the answer. If length of the answer entered by user is above the configured value then validation will fail and user will get configured error message.
Date	Date/Time pattern string for the answer. For example, pattern can be "MMddyy" for Month Day Year validation. If the date/time answer entered by user is not as per the configured pattern then validation will fail and user will get configured error message.
Regex	Regex pattern string for the answer. For example, pattern can be "[A-Za-z0-9]+" for Alpha-numeric validation. If the answer entered by user is not as per the configured regex pattern then validation will fail and user will get configured error message.
Repeated Character	Allowed number of repeated characters in the answer. If the answer entered by user is containing repeated characters more than the configured value then validation will fail and user will get configured error message.

Table 9–1 (Cont.) Validation Parameters

Validation Scheme/Type	Description for Validation Parameter
Repeated Answers	Allowed number of repeated answers. For example parameter value can be '1' for Unique answer validation. If the answer entered by user is repeated more than configured number of times then validation will fail and user will get configured error message.

9.3.2 Editing Existing Validation

To edit existing validation

1. On the Admin menu point to KBA, then Questions and then click Validations.

   The Validation List/Editor page appears

2. Click the Validation name which you want to edit.

   The Validation customization section appears above the list of validations.

3. Make necessary changes in Validation Parameters. See Table 9–1, " Validation Parameters".

   The Validation customization section allows user to edit Name, Allowed Characters, and Error Message fields.

4. Click Save

   Adaptive Risk Manager Online updates this validation instance in the system.

9.3.3 Importing Validations

To import validations

1. On the Admin menu, point to KBA, point to Questions, and then click Import Validations.

   The Import Validations page appears.

2. Click Browse and locate the Zip file of validations you want.

3. Click Import.

   The Import Validations page appears with a list of the newly imported validations.

9.3.4 Exporting Validations

To export validation(s)

1. On the Admin menu point to KBA, then Questions and then click Validations.

   The Validation List/Editor page appears.

2. Click the check box next to each validation you want to export.

   Toggle button "Select All" helps select/deselect all the validations.

3. Click Export button available above/below the list of validations.

4. Click OK to the confirmation.

   The Open dialog box appears.

5. Click Save To Disk and then click OK.

The select validation(s) are exported.

9.3.5 Deleting Validations

To delete validation(s)

1. On the Admin menu point to KBA, then Questions and then click Validations.

   The Validation List/Editor page appears.

2. Click the check box next to each validation you want to delete.

   Toggle button "Select All" helps select/deselect all the validations.

3. Click Delete button available above/below the list of validations.

4. Click OK to the confirmation.

   The select validation(s) are deleted.

9.4 Configuring the Registration Logic

In the Registration Logic area you can manage and configure the registration for challenge questions and answers. To do so, you enter values for the Question Set generation and any global validations needed.

To view and configure the registration for challenge questions and answers

1. On the Admin menu, point to KBA, point to KBA Logic, and then click Registration Logic.

   The Registration Logic page appears.

2. To enter or change the values for the question set generation, enter a value in the appropriate field at the top of the page.

   You can specify the:

   - Number of questions that a user needs to register
   - Number of questions that appear on each menu
   - Number of categories per menu

   Note: Enter realistic numbers. For example, the number of questions that a user needs to register should be 3 to 5 questions

3. To add global validations, in the Available Validations box, click the validation you want to add and then click Add.

   The validation appears in the Global Validations box.

4. To delete a global validation, in the Global Validations box, click the validation you want to delete and then click Delete.

5. Click Save.

9.5 Configuring the Answer Logic

The KBA answer logic configuration screen includes controls for the level of each Answer logic algorithm used for answer validation. The higher the level the less exact answers need to be for acceptance.

You can configure the answer logic (fuzzy logic) algorithms on the Answer Logic page. The algorithms are divided into three categories: Common Abbreviations, Fat Fingering (accidentally pressing the nearest neighbor on the keyboard), and Phonetics.

1. On the Admin menu, point to KBA, point to KBA Logic, and then click Answer Logic.

   The Answer Logic page appears.

2. Click in the Authentication Type box and specify whether you want the configuration to apply to the Online challenge or CRS Phone Challenge.

   You can specify different settings for online and phone challenge.

3. To change the level of answer logic used for a category, select Off, Low, Medium, or High: the lower the setting the higher degree of exactness required.

4. Click Save.

9.5.1 Adjusting the Level of Answer Logic

The level of Answer logic used to evaluate answers given for challenge questions is adjustable through Adaptive Risk Manager. You can enable or disable each algorithm. In addition, you can also specify the following level of algorithm used:

- Off – No Answer logic is used; answers must exactly match those previously registered by the user.
- Low – Less Answer logic; answers must be more exact
- Medium – More Answer logic
- High – Highest level of Answer logic

Each algorithm generates a score that represents how close the given answer is to the registered answer. Adaptive Risk Manager can be configured to accept different threshold score ranges for each algorithm individually. Separate threshold values for each algorithm (low/medium/high) are set in a properties file. Below are the default thresholds.

Abbreviation:

- Return values: 0 or 100 (no-match OR match)
- Levels: OFF, LOW (100), MEDIUM (100), HIGH (100)
- Logic
  - If an abbreviation entry exists linking the given strings, score is 100
  - Else score is 0

Fat finger:

- Return values: range 0 to 100
- Levels: OFF, LOW (90+), MEDIUM (75+), HIGH (60+)
- Logic
  - If the string lengths don't match, score is 0
  - If a position does not have the expected character or its neighbor, score is 0
  - Else compute the number of positions that have the neighboring characters.
  - Score = (StringLength – NeighborPositionCount) * 100 /StringLength

Phonetics:

- Return values: 0, 60, 75, 90
- Levels: OFF, LOW (90), MEDIUM (75), HIGH (60)
- Logic
  - Compute primary and alternative phonetic keys for the given strings, using DoublMetaphone algorithm
  - If primary keys of both strings match, score is HIGH
  - Else if a primary key of one of the strings and alternate key of the other string match, score is MEDIUM
  - Else if the alternate keys of both string match, score is LOW
  - Else the score is 0

Multiple word answers

Answers that contain multiple words are treated in a specific way by the answer logic. If the final score from a complete string match does not meet the "success" criteria, individual words in the answer are evaluated. If each individual word in an answer is accepted by any of the algorithms the whole answer is accepted.

Multiple word answers with missing/extra words must be an exact match to the registered answer. Answers must have the same number of words as the registered answer to be evaluated with Answer logic.

For example: If the registered answer is "Mead Elementary School" and the answer given at the time of challenge is "Mesd Elem Sch":

```
Abbreviation: Mead-Mesd=0; Elementary-Elem=100; School-Sch=100
Fat-finger: Mead-Mesd=75; Elementary-Elem=0; School-Sch=0
Phonetics: Mead-Mesd=0; Elementary-Elem=0; School-Sch=0
```

Let's assume that abbreviation was set to anything besides off and fat fingering was set to medium or high. Since all three words would be accepted individually the whole answer would be accepted.

9.5.2 Answer Logic Hints

A hint can be added to questions individually to affect the answer logic used to evaluate given answers. This is done to better tune the logic for the type of question. This is especially important for date related questions.

For example, if a question has the date answer hint applied then the abbreviations, phonetics and fat fingering answer logic will run first then special date format logic will be applied.

9.6 KBA Security Solution Guidelines and Recommended Requirements

These recommendations provide guidelines for implementing KBA authentication. They provide guidance to institutions for configuring and implementing custom enrollment and challenge procedures within the guidelines of best practices.

9.6.1 Questions Guidelines

- No confidential data used in question.

- Answers are difficult to guess.
- Answers cannot be obtained from public sources.
- Questions that are applicable to general public.
- Answers are memorable/personally significant.
- Questions where answers can change over time are avoided.
- Questions cannot pertain to religion, politics, taboo subjects, and so on.

9.6.2 Answer Guidelines

- Answers must be at least 4 characters.
- No more than 2 answers can be the same during registration.
- Answers cannot have more than 2 repeating characters.
- Special characters are not allowed.
- Answers are not case sensitive.
- Extra white spaces are removed.
- Fuzzy logic implemented - degree configurable by client.

9.6.3 Business/Security Recommended Requirements

- Unique pick set for each customer.
- Register 3-5 questions. i.e. 15 total questions to select from, 3 drop down menus of 5 questions each.
- Maximum of 2 questions from the same category in a drop-down menu.
- Maximum opt-out - i.e. 3 opt-out attempts before "force" registration.
- When challenged, the same question is to be presented until user responds correctly or question is reset by customer service agent.

9.7 Questions about Collection and Challenge

Can KBA collection be limited to low-risk transactions?

KBA registration can be deferred if the login conditions are risky. The administrator can update the registration model based on his requirements.

How can an administrator configure the system so that if a user continues to come from a high-risk location, and so on, he will be blocked after a defined time period and collection will be performed by a customer service representative?

The administrator can add a new action—for example "risky_session"—and add a rule—for example "action count"—to force a block after a specified number of risky sessions?

How can the administrator configure the system so that the user can choose to skip the collection process "n" number of times?

The administrator will need to add a rule—for example, "action count"—and force registration after a specified number of skips.

9.8 Best Practices for Managing Challenge Questions

- Many validations may be applied locally or globally. You must be careful not to apply any validations globally that you do not want to influence all answer registration. For example, if the "Four digit year (YYYY)" validation is applied globally then only for numeral answers will be accepted during KBA registration. This would be a problem if there are questions available to users that would normally have alphanumeric answers.
- You can create, edit, and delete questions and categories. You should take care when deleting categories and questions. Insufficient numbers of questions and categories can impact the security of the solution and cause usability issues. For example, if the "Categories per menu" registration logic is set to a number that is more than the total number of categories in the system then there may be duplicate questions listed. This can be confusing to end users so it should be avoided.
- For security and usability reasons set the "Questions per menu" setting between 4 and 7. This range provides a good mix of questions in a user's question set but does not expose too many questions to any single user.
- The "Questions user will register" setting should be between 3 and 5. This provides enough questions to offer good security but does not over burden a user's memory. The basic industry standard for KBA is 3 registered questions.
- It is recommended that you completely configure all of the challenge questions, including locale, before making the question available to customers.
- If you disable a challenge question, customers who previously had that question will continue to have the question even after it is disabled. However, users that are registering for the first time or re-registering will not be presented with the disabled question.

Part III

Cases

This part provides an overview of cases and step-by-step procedures for creating and managing cases.

Part III contains the following chapter:

- Chapter 10, "Cases"

10

Cases

Oracle Adaptive Access Manager provides a set of tools for creating and supporting two different types of cases: Customer Service Representative (CSR) Cases and Agent Cases.

CSR Cases are used in customer care situations associated within the normal course of doing business online and over the phone when providing assistance to customers. The customer support representatives can use the CSR set of tools for handling inquiries associated with adaptive risk manager.

Agent Cases are used specifically by fraud investigators and investigation managers for analyzing data and finding relationships between sessions and cases. When an investigator links sessions and cases, Oracle Adaptive Access Manager can search the data for suspicious activity.

This chapter provides information about CSR cases and Agent cases, case dispositions, and case workflow.

10.1 Managing Cases

The procedures for managing CSR and Agent cases are identical for searching and closing cases, changing a case's status and severity level, and adding notes.

10.1.1 Searching Cases

Oracle Adaptive Access Manager provides the Search User Cases page to quickly locate a CSR case or an Agent case in the system. You can search the list by Application ID, username, case number, keyword, or date range. You can also filter the list by severity level, case status, disposition, or expired/overdue.

After you locate the case you want, you can click the case ID to view the case details.

When you have located a specific case or created a new case, you have the option of performing several different tasks. The Search Cases page also enables you to create a new CSR or Agent case.

To view a list of all CSR cases

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. To locate cases for a specific end user, enter the User Name.
3. To locate a specific case, enter the case number.

4. To locate a case by a keyword that appears in the description, enter the word you want.
5. To locate cases by the date in which the last action occurred or by case create date, click the calendar icons and then click the start and end dates you want.
6. To filter the list by case severity level, select the severity level you want.

   The severity level is a marker to communicate to case personnel how severe this case is. The severity level is set by whomever creates the case. The available severity levels are High, Medium, and Low. If a customer suspects fraud, then the severity level assigned is "High." If the customer wants a different image, then the severity level assigned is "Low." Severity levels of a case can be escalated or de-escalated as necessary.
7. To filter the list by case status, select the status you want.

   Status is the "current" state of a case. Status values used for a case are New, Pending, or Closed. When a case is created, the status is set to New by default.
8. To filter the list by case type, select the type you want.

   CSR - CSR cases are used in customer care situations associated within the normal course of doing business online and over the phone when providing assistance to customers.

   Agent - Agent cases that fraud investigators and investigation managers work on. They are used specifically by fraud investigators and investigation managers for analyzing data and finding relationships between sessions and cases.
9. To filter the list by disposition, select the disposition you want.

   The disposition describes the way in which the issue was resolved in a case. Cases only have dispositions when they're closed. If a case has any status besides closed, the disposition is left blank.

   The dispositions to choose from are:

   - Confirmed Fraud
   - Duplicate
   - False Negative
   - False Positive
   - Issue Pending
   - Issue Resolved
   - Not Fraud
10. To filer the list by expired/overdue, select the option you want.

    The options available are:

    - Show All
    - Hide
    - Show Only
11. Click Run Query.

10.1.2 Bulk Editing

The Search User Cases page enables you to change the Severity, Status, and Expiration Date settings for multiple cases at once.

To change the case settings for multiple cases at once:

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.
2. Select the check box next to each case you want to edit.
3. Click Edit Cases.

   The Edit Cases page appears.
4. Change the case settings you want and click Apply Edit.

10.1.3 Closing Multiple Cases

To close multiple cases at once:

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.
2. Select the check box next to each case you want to close.
3. Click Edit Cases.

   The Edit Cases page appears.
4. Choose Closed for the Case Status and click Apply Edit.

10.2 CSR Cases

This section provides information about viewing, creating, and specifying the disposition of a CSR case.

Customer Service personnel can access various functionality in Adaptive Risk Manager based on the role to which they are assigned. The default, built-in roles include Customer Service Representative and Customer Service Representative Manager.

- Customer Service Representative

  CSRs have very limited access to Adaptive Risk Manager. CSRs have access to search, open, and create CSR type cases. There are no outward facing hyperlinks in any of the screens CSRs have access to. CSRs have access to a limited list of actions and no access to bulk edit functions on the Search User Cases page.
- Customer Service Representative Manager

  CSR Managers have the access privileges of CSRs and some other limited functionality. Members cannot create Agent cases, and hide Actions, Log, and Linked/Related tabs in Agent cases.

10.2.1 Creating a New CSR Case

A CSR case is a record of related customer care events and actions for a single customer. Multiple cases also provide a way of segregating unrelated issues and actions for a customer.

CSR cases are used by the customer service representative while assisting a customer.

To create a new CSR case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Enter your User Id or User Name and Application ID (if applicable) at the top of the page.
3. Enter a description of the case at the top of the page.
4. Select CSR from the Case Type menu at the top of the page.
5. Select a severity level from the Severity Level list at the top of the page.
6. Click Create Case.

   The Case Details page appears and displays the logins for that user.

10.2.2 Actions

You can take action in a CSR case to add notes, reset challenge questions, change the severity level or status of a case, escalate a case, enable a temporary allow, reset the image and phrase, or extend expiration date for a case.

10.2.2.1 Changing a Case's Status

Status refers to the current state of a case, to whether it is new, pending, or closed. Adaptive Risk Manager Online automatically assigns the status of "New" to each case when it is created. You need to change the status to Pending once the case is escalated.

To change the status of a case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case Details page appears and defaults to the Logins tab

3. Click the Actions tab.
4. In the Action list, click Change Status.

   The Status list appears below the Action list with contextual instructions.

5. In the Status list, click the status you want.

   You can select New, Pending, or Closed.

6. If you select Closed, the dispassion menu appears from which you need to select the reason why you are closing the case.
7. Enter a note describing why you are taking the action.

   You can select from existing notes or enter a new note.

8. Click Submit.

10.2.2.2 Adding a Note to a Case

Each time you take an action in a case you are required to enter a note describing why you are taking the action. You can also select the action "Add Note" with the express purpose of adding a note to a case. In this instance, you can either add a "Standard" note that can be written and read by customer service representatives, managers, and

investigators; or you can add a "Restricted" note that can only be written by investigators and read by customer service managers and investigators.

To add a note to a case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case Details page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Add Notes.

   The Notes field appears to the right.

5. Enter a note.

6. Click Submit.

10.2.2.3 Changing the Severity Level of a Case

When a case is created it is assigned a severity level to indicate its importance. The severity level is shown on the Case Details page. The available severity levels are High (Red), Medium (Yellow), and Low (Blue). If a customer suspects fraud, then the severity level assigned would be High. If the customer wants a different image, then the severity level assigned would be Low. You can escalate or de-escalate the severity level of a case as necessary.

To escalate or de-escalate the severity level of a case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Change Severity.

   The Severity list appears below the Action list.

5. In the Severity list, click the severity level you want.

6. Enter a note describing why you are taking the action.

   You can select from existing notes or enter a new note.

7. Click Submit.

10.2.2.4 Resetting a Customer's Personal Information (KBA)

Authenticator uses images and phrases on its virtual authentication devices as part of the personalization to help prevent fraud. During phone contact with a customer you can reset their personal image and/or phrase. Authenticator also uses questions as additional credentials to help prevent fraud. You can reset these questions for the customer when necessary.

The Action tab on the Case page enables you to reset the following personal items for a customer:

- Image—Randomly assigns a new image to the customer.
- Phrase—Randomly assigns a new phrase to the customer.
- Image & Phrase—Randomly assigns a new image and phrase to the customer.
- Customer (All)—Deletes the customer's image, phrase, questions and question set. The customer will be sent through the registration flow the next time they log in.
- Reset Questions—Deletes the current questions and answers. The customer will need to select new questions and answers form their question set the next time they log in.
- Next Question—Advances the customer to the next challenge question in their list of registered questions. So if they are currently being asked question A, they will now be asked question B or C.
- Reset Question Set—Deletes the current questions and answers and generates a new question set for them to register from.
- Unlock Customer—If a customer is locked out of the system as a result of failed challenge questions, Unlock Customer resets the customer's failure counter.
- Ask Question—Displays a challenge question for the CSR to ask the customer and a field to enter customer's response.

To reset a customer's image

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.
4. In the Action list, click Customer Resets.

   The User Item list appears below the Action list.

5. In the User Item list, click Image.

   The Notes list appears.

6. In the Notes list, click the note you want.
7. If you select "Other" from the Notes list, enter a note describing why you are taking the action.
8. Click Submit.

   Adaptive Risk Manager Online generates a new image. Inform the customer that they will see a new personal image in their Authenticator the next time they login to the Web site but their phrase will be unchanged.

To reset a customer's phrase

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click Actions.

4. In the Action list, click Customer Resets.

   The User Item list appears below the Action list.

5. In the User Item list, click Phrase.

6. In the Notes list, click the note you want.

7. If you selected "Other" from the Notes list, enter a note describing why you are taking the action.

8. Click Submit.

   Adaptive Risk Manager Online generates a new phrase. Inform the customer that they will see a new security phrase in their Authenticator the next time they login to the Web site but their personal image will be unchanged.

To reset a customer's image and phrase

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Customer Resets.

   The User Item list appears below the Action list.

5. In the User Item list, click Image & Phrase.

6. In the Notes list, click the note you want.

7. If you selected "Other" from the Notes list, enter a note describing why you are taking the action.

8. Click Submit.

   Adaptive Risk Manager Online generates a new image and phrase. Inform the customer that they will see a new personal image and security phrase in their Authenticator the next time they login to the Web site.

To reset a customer's security questions, question set, image, and phrase

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case Details page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Customer Resets.

   The User Item list appears below the Action list.

5. In the User Item list, click Customer (All).

6. In the Notes list, click the note you want.

7. If you selected "Other" from the Notes list, enter a note describing why you are taking the action.

8. Click Submit.

Adaptive Risk Manager Online resets the customer's security questions, question set, image and phrase. Inform the customer that they will go through security registration the next time they login to the Web site.

To reset a customer's questions

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Challenge Questions.

   The Item list appears below the Action list.

5. In the Item list, click Questions.

6. In the Notes list, click the note you want.

7. If you selected "Other" in the Notes list, enter a note describing why you are taking the action.

8. Click Submit.

   Adaptive Risk Manager Online deletes the existing questions and answers. Inform the customer that they will go through security questions registration the next time they login to the Web site.

To increment a customer to their next question

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Challenge Questions.

   The Item list appears below the Action list.

5. In the Item list, click Next Question.

6. In the Notes list, click the note you want.

7. If you selected "Other" in the Notes list, enter a note describing why you are taking the action.

8. Click Submit.

   Adaptive Risk Manager Online allows the customer to proceed to the next question. Inform the customer that they will be asked a different security question the next time they login to the Web site.

To reset a customer's security questions and the set of questions to pick from

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.
4. In the Action list, click Challenge Questions.

   The Item list appears below the Action list.
5. In the Item list, click Reset Question Set.
6. In the Notes list, click the note you want.
7. If you selected "Other" from the Notes list, enter a note describing why you are taking the action.
8. Click Submit.

   Adaptive Risk Manager Online resets the customer's security questions and the set of questions they may register questions from. Inform the customer that they will go through security questions registration the next time they login to the Web site.

To unlock a customer (KBA)

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.
2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.
3. Click the Actions tab.
4. In the Action list, click Challenge Questions.

   The Item list appears below the Action list.
5. In the Item list, click Unlock Customer.
6. In the Notes list, click the note you want.
7. If you selected "Other" from the Notes list, enter a note describing why you are taking the action.
8. Click Submit.

To extend expiration date

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.
2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.
3. Click the Actions tab.
4. In the Action list, click Extend Expiration Date.

   The Extension list appears below the Action list.
5. In the Extension list, choose the length of time you want the expiration to be extended to.
6. In the Notes list, click the note you want: Extended or Other.
7. If you selected "Other" from the Notes list, enter a note describing why you are taking the action.
8. Click Submit.

To use a customer's challenge questions for phone authentication

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Challenge Questions.

   The Item list appears below the Action list.

5. In the Item list, click Ask Question.

   A challenge question appears in the Question field.

6. Ask the customer the question.

7. Enter the customer's answer in the Answer field.

8. In the Notes list, click the note you want.

9. If you selected "Other" from the Notes list, enter a note describing why you are taking the action.

10. Click Submit.

    If the customer answers the question correctly, the system automatically takes appropriate action depending on their status such as unlocking the customer if they were locked out.

    If the customer answered the question incorrectly, they will get additional attempts at that question (depending on configuration). If the customer exceeds the maximum number of failures for a question another question appears in the Question field. If you ask the customer two or more questions in this process, and they answer successfully, their questions are automatically reset.

    If you ask all of the questions and the customer failed all attempts at each question, the customer will be locked out of online access.

10.2.2.5 Enabling a Temporary Allowance

A customer may be blocked from logging in or performing transactions if a security rule is being triggered. For example, they may be traveling on business and attempting to log in from a black listed country and the system has blocked them. You can use the Temporary Allow feature to grant temporary account access to a customer who is being blocked from logging in or performing a transaction.

To allow a blocked customer temporarily

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Temporary Allow.

   The Allow list appears below the Action list.

5. In the Allow list, select the desired temporary allow.

6. If you select "Select End Date", click the calendar icon and click the end date you want.
7. Click in the Notes box and select the type of note you want.

   If you want to terminate an active allow for a customer, select Cancel to remove it
8. If you selected Other as the note type, enter a note describing why you are taking the action.
9. Click Submit.

10.2.2.6 Unregistering a Device

Your customers can elect to register their device during registration. A customer might, for example, register their office or home computers, but not register a computer they might use on a business trip.

The rules administrator could then write or configure rules based on a device registered flag. For example, they could configure a rule that would always challenge the customer if their current device is not registered. Or they could create a larger rule that would take the fact that the device is not registered into account.

As a CSR you can unregister all of a customer's devices through the Actions tab on the Case Details page.

To unregister a customer's devices

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.
2. Click the case number of the case you want.

   The Case Details page appears and defaults to the Logins tab.
3. Click the Actions tab.
4. In the Action list, click Customer Resets.

   The User Item list appears below the Action list.
5. In the User Item list, click Unregister Devices.
6. In the Notes list, click the note you want.
7. If you selected "Other" from the Notes list, enter a note describing why you are taking the action.
8. Click Submit.

   All of the customer's devices are unregistered.

10.2.3 Case Activity Log

Adaptive Risk Manager Online maintains a unique log of every customer service action taken while working on a case. Each log entry includes the log ID, CSR user ID, log code, and notes. You can use this Log while you are in phone contact with a customer to view the case history.

You can search the log of a case by CSR user ID, notes keyword, date range, or action keyword. You can also filter the log by log code.

To view a log of all activity within a case

1. Click Search Cases on the Cases menu.

The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Log tab.

   The activity log for that case appears at the bottom of the page.

To search the log of a case

1. Display the log for the case you want to search.
2. Enter search criteria in the fields for CSR ID, Notes Keyword, Action Keyword, or date range.
3. Click Run Query.

To filter a log by log code

1. Display the log for the case you want to filter.
2. In the Log Code list, select the log code you want.
3. Click Run Query.

10.2.4 Customer's Logins

When you are in telephone contact with a customer you can view a list of that customer's previous logins. The list of logins provides information about authentication status, login time, device ID, location, and alerts.

To view a list of a customer's logins

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

   The list of past logins for that case appears at the bottom of the page.

To search for a customer's logins by device ID or date range

1. Display the list of logins for the case.
2. To search the log by device ID, enter the ID of the device.
3. To search the log by date range, click the calendar icons and select the start date and the end date.
4. Click Run Query.

To filter the list of customer's logins by authentication status or alert level

1. Display the list of logins for the case.
2. To filter the log by authentication status, select the authentication status you want.
3. To filter the log by alert level, select the alert level you want.
4. Click Run Query.

10.2.5 Case Details

By clicking the case number on the Search User Cases page, you can open an existing case. The case page provides such general details about the case as the customer's user name, status, severity level, and description. It also provides access to the actions that can be taken, a log of case activity, and a list of customer logins.

10.2.5.1 CSR Case Details

To view the case details, click the plus sign (+) next to Case at the top of the page.

The following information will be displayed in Case Details.

General Case Details

- Case Created - The date and time the case was created.
- Case Status - The case status can be New, Pending, or Closed. When a case is created, the status is set to New by default.
- Severity Level - The severity level is set by whomever creates the case and used as a marker to communicate to users how severe this case is.
- Case Type - Agent or CSR
- Disposition - When a case is closed the disposition describes the way in which the issue was resolved. Cases only have dispositions when they're closed. If a case has any status besides closed, the disposition is blank.
- Expiration Date: Date when CSR case expires. By default, the length of time before a case expires is 24 hours. After 24 hours, the status will change from New to Expired. After the case expires, the CSR user will not be able to open the case anymore, but the CSR manager will be able to. The length of time before a case expires is configurable in the customercare.properties file. Refer to the *Oracle Adaptive Access Manager Developer's Guide* for details for configuring the expiry behavior.
- Description - The details for the case. A description is required.
- Last Case Action - The last action executed for this user in the CSR case
- Date of Last Case Action - The date when last action occurred.
- Last Global Case Action - The last action that occurred for this user (identified by a combination of the Username and User ID) in ALL CSR cases. Agent cases are not taken into account.
- Date of Last Global Case Action - The date when the last action was perform against the user online.

User Data

- Username - User for whom case is created
- User ID - Encrypted username
- Application ID - The ID of the application.

  In a multi-tenant deployment, CSRs will only have access to cases limited to their primary Application ID. CSR Managers and investigators can access cases from multiple applications.
- Last Online Action - The last action that user executed, for example - Answered challenge question would show "Challenge Question" or if user is blocked, "Block."

- Date of Last Online Action - Date when last online action was executed.
- Temporary Allow Expire Date - When temp allow is enabled; this field tells you when it expires. If temporary allow is 7 days, the expiry date will be a week from today.
- Temporary Allow Active - If temporary allow is active, this field shows "Yes;" otherwise the field shows "No."
- Completed Registration - If user has completed registration, this field shows "Yes;" otherwise it shows "No." The user must complete all of the following tasks: personalizing a TextPad (image and phrase), and registering security questions and answers.
- Questions Active - If user has completed registration, but questions have been reset, and he hasn't gone back and registered new ones, this field would display "No." This field shows "yes" if the user has completed registration and questions exists by which he can be challenged.
- Personalization Active - When user has an image, a phrase and questions active, this field would display "Yes." If any one of these are reset, this field would display "No."

10.2.5.2 Viewing Details about Logins and Actions

Instructions to view details about logins, a log of actions, or a list of available actions are given below.

To view details about logins

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case Details page appears which displays details about the case at the top and a list of the recent logins at the bottom.

To view a log of actions on this case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case Details page appears.

3. Click the Log tab.

To view a list of actions available for a case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case Details page appears.

3. Click the Actions tab.

10.2.6 User ID Details

By clicking the user ID on the Search User Cases page, you can open the User ID Details page for an existing case. The page provides such general details about the user as the user name, user group, and application ID. It also provides access to details about the user group, devices associated with the user ID, locations associated with the user ID, alerts associated with the user ID, and so on.

10.3 Agent Cases

Agent cases are tools for investigators and investigation managers to facilitate an investigation by identifying the data and relationships. By linking sessions and cases so that Oracle Adaptive Access Manager case locate relationships or related cases to the data that is linked in those sessions, sessions in which an suspicious activity has occurred, a session in which an alert was generated.

10.3.1 Creating a New Agent Case

This section provides information about viewing, creating, linking cases, and specifying the disposition of an agent case.

To create a new agent case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Enter a description and choose a severity level. Agent cases are not associated with a particular user. Agent cases can be created with just a description and severity level, and so, they do not need a username or User ID. Enter your User ID or Username and Application ID (if applicable) at the top of the page.

3. Select Agent from the Case Type menu at the top of the page.

4. If you want, enter your User ID, Username, and Application ID (if applicable). Agent cases are not associated with a particular user. Agent cases can be created with just a description and severity level; therefore, they do not need a User ID or Username.

5. Click Create Case.

   The Case Details page appears and displays the login sessions for that case.

Once the Agent case is created, any number of sessions can be selected for linking to the new Agent case. These sessions are the basis for the new case relationships.

10.3.2 Agent Case Details

The Case Details page provides such general details about the case as the customer's user name, status, severity level, and description.

To view the case details, click the plus sign (+) next to Case at the top of the page.

The following information will be displayed in Case Details.

- Case Created - The date and time the case was created.
- Case Status - The case status can be New, Pending, or Closed. When a case is created, the status is set to New by default.
- Severity Level - The severity level is set by whomever creates the case and used as a marker to communicate to users how severe this case is.

- Case Type - Agent or CSR
- Disposition - When a case is closed the disposition describes what the resolution was. If a case has any status besides closed the disposition is blank.
- Expiration Date - Date when agent case expires. An agent case becomes overdue if not accessed by that date. Once the case is accessed, the expiration date will be reset to the new value and the case is active.
- Overdue - If a case is open and has not been accessed longer than the time range set the overdue flag will be set to allow managers to see cases needing attention. For example, if Agent cases are set to 24 hours then the flag will be set to "overdue" if a case is open and has not been accessed in more than 24 hours. An overdue case will be refreshed for another 24 hours if an investigator accesses it. The overdue behavior is configurable in the customercare.properties file. Refer to the *Oracle Adaptive Access Manager Developer's Guide* for details.
- Description - description of the case.
- Last Case Action - The last case action executed for this Agent Case. There are no user details in agent cases.
- Date of Last Case Action - Date when last case action was executed.

10.3.3 Link Sessions

Sessions and/or data that you feel has specific importance to a case may be linked to a case.

The Link Sessions tab on the Case Details page displays a list of login sessions for the case you are investigating. You can search the list by entering search criteria to quickly find the desired login sessions. When found, you can link the sessions to the case to find relationships. You can link as many sessions as you think might be connected to an investigation, but at least one linked session must exist in order for linked sessions to be meaningful.

To find the login sessions you want

1. On the Case Details page, click the Link Sessions tab.
2. To filter sessions by authorization status, select the status you want from the Authorization Status menu.
3. To filter sessions by client type, select the type you want from the Client Type menu.
4. To filter sessions by alert level, select the alert you want from the Alert Level menu.
5. To locate sessions by Application ID, User ID, Username, Device ID, IP Address, Session ID, or Internal Session ID, enter the search criteria in the appropriate field.
6. To locate sessions within a specific time frame, click the To and From calendar icons and select the start and end dates you want.
7. Click Run Query.

To link sessions to cases

You can link sessions to cases. For example, an investigator could identify three sessions which were found to contain similar fraud. The sessions could be selected from a query and linked to an existing case.

1. Select the check box next to each session you want to link.

2. Click the plus sign (+) next to Enter Linking Notes at the top of the page and enter the notes you want about why you are linking the sessions.
3. Click Link.

   The Linked/Related tab appears.

10.3.4 Linked/Related

The Linked/Related tab provides four panels that display the linked sessions, related data types, related sessions, and related cases.

After you have linked the sessions you can select the data within the sessions that you want to use for finding relationships.

Related data points are highlighted in red.

10.3.4.1 Linked Sessions

The Linked Sessions panel displays all of the sessions that you linked. By default all of the sessions and data points within the sessions are preselected. The panel enables you to select and deselect the sessions and data points within those sessions that you want to use to build relationships.

In addition to the basic session information that Oracle Adaptive Access Manager uses to build relationships such as username, device ID, and location, you can also use transaction information, if it is available. You can include transaction entities such as shipping address and credit card number, which appear in the Transaction column, to find related data in sessions not included in the linked sessions.

To specify the data points you want

1. Select or deselect individual data points such as User ID, Username, Device ID, or IP Address that you want to include or exclude.

   The related data points are displayed in red.
2. Click Refresh Relationships.

The data points selected in Linked Sessions are used as the foundation for relationships; they are used in the calculation of related cases and sessions. These data points will be highlighted in related sessions and related cases.

To unlink a sessions

1. Click to clear the check box next to the session you want to unlink.
2. Click the plus sign (+) next to Enter Linking Notes and enter notes about why you are unlinking the session.
3. Click Unlink.

10.3.4.2 Related Data Types

The Related Data Type panel enables you to specify what types of data you want to use to create relationships. Selecting related data types is the same as selecting data points in Linked Sessions except that Transactions and Alerts are available choices in Related Data Types.

To specify the data types you want to include

1. Select the check box next to the data types you want: user ID, username, device ID, IP address, alerts, or transactions.

2. Click the plus sign (+) next to Enter Linking Notes and enter notes.
3. Click Link.
4. Click Refresh Relationships

To specify particular values for the data types

1. On the Filter Related Sessions/Cases panel, enter the values you want in the data type fields.
2. Click Refresh Relationships.

10.3.4.3 Related Sessions

Sessions that share data with the linked sessions are related and displayed in the Related Sessions panel. This panel enables you to link these cases to the ones in Linked Sessions.

To specify the sessions you want to link to the case

1. Select the sessions you want to link.
2. Click the plus sign (+) next to Enter Linking Notes and enter notes.
3. Click Link.
4. Click Refresh Relationships.

10.3.4.4 Related Cases

Cases that share data with the linked sessions are related and are displayed in Related Cases. Search parameters are available to further narrow the view. The cases will display the data points by which they are related. Each case number will contains links to the case. If there is another investigation in progress that is related to this one, you can define related cases in the Related Cases panel.

To specify the cases you want to include

1. Select the cases you want to include.
2. Click the plus sign (+) next to Enter Linking Notes and enter notes.
3. Click Link.
4. Click Refresh Relationships.

10.3.5 Log

The Log tab displays a list of actions taken on the case to date and includes the log ID, CSR ID, date, log code, and notes.

10.3.6 Actions

You can take action in an agent case to add notes, change the severity level of a case, or change the status of a case.

10.3.6.1 Adding a Note to a Case

Each time you take an action in a case you are required to enter a note describing why you are taking the action. You can also select the action "Add Note" with the express purpose of adding a note to a case.

To add a note to a case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case Details page appears.

3. Click the Actions tab.

4. In the Action list, click Add Notes.

   The Notes field appears to the right.

5. Enter a note.

6. Click Submit.

10.3.6.2 Changing the Severity Level of a Case

When a case is created it is assigned a severity level to indicate its importance. The severity level is shown on the Case Details. The available severity levels are High (Red), Medium (Yellow), and Low (Blue). You can escalate or de-escalate the severity level of a case as necessary.

To escalate or de-escalate the severity level of a case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Change Severity.

   The Severity list appears below the Action list.

5. In the Severity list, click the severity level you want.

6. Enter a note describing why you are taking the action.

   You can select from a list of existing notes or enter a different note.

7. Click Submit.

10.3.6.3 Changing the Status of a Case

You can change the status of a case to indicate new, pending, or closed. If you close a case you need to select the disposition indicating why the case is being closed.

To change the status of a case

1. Click Search Cases on the Cases menu.

   The Search User Cases page appears.

2. Click the case number of the case you want to view.

   The Case page appears and defaults to the Logins tab.

3. Click the Actions tab.

4. In the Action list, click Change Status.

The Status list appears below the Action list.

5. In the Status list, click the status you want.
6. If you select Closed, the Disposition menu appears from which you need to select the reason for closing the case.
7. Enter a note describing why you are taking the action.

   You can select from a list of existing notes or enter a different note.
8. Click Submit.

Part IV

Dashboard and Reporting

This part provides information on using the dashboard for online and offline monitoring and investigation, monitoring alerts, running queries, and scheduling and exporting a report. It also provides information on using Oracle BI Publisher as the reporting solution for Oracle Adaptive Access Manager.

Part IV contains the following chapters:

11

Using the Dashboard

The Oracle Adaptive Access Manager Dashboard is an application that provides a high-level view of real customer data, presenting:

- performance statistics
- expanded summary data
- statistics based on location, scoring, device, security, and performance

This chapter provides detailed instructions on how to use the dashboard.

11.1 Introduction

11.1.1 What is a Dashboard

The Oracle Adaptive Access Manager dashboard is a unified display of integrate information from multiple components into a user interface that organizes and presents data in a way that is easy to read.

Dashboard reports that are presented help you visualize and track trends. With a dashboard report you could check the frauds/alerts in your system. The dashboard also helps you make decisions based on user/location/devices profile allowing easy identification of risks taking place in the system.

11.1.2 Dashboard for Adaptive Risk Manager Online and Offline Applications

In Adaptive Risk Manager Online, the Dashboard uses real-time data in the system at the current moment and historically, and in Adaptive Risk Manager Offline, the Dashboard uses existing customer data from Adaptive Risk Manager Online or from a remote source.

In an online production system, the user is primarily interested in the performance and summary panels.

In an offline system, the user is primarily interested in the dashboard section for historical data.

11.1.3 Common Terms and Definitions

This section contains common dashboard terms and definitions.

- Refresh - the rate to update Dashboard with new data. The choices are 30 seconds, 1 minute, and 10 minutes.

- Performance Panel - The top panel of the Dashboard that shows current data.
- Summary Panel - The middle panel of the Dashboard that shows aggregate data.
- Dashboard - The bottom panel of the Dashboard that shows historical data.
- Data type - Type of information in the Oracle Adaptive Access Manager system.
- Range - The time frame. The choices are Today, Last 1 day, Last 7 days, Last 30 days, and Last 90 days.
- Average Process Time - Average number of milliseconds for execution.
- Blocked Logins - Logins that were blocked during the login runtime.
- Blocked Transactions - Transactions that were blocked during the transaction runtime.
- High Alert (Logins) - High level alerts triggered during the login runtime.
- High Alert (Transactions) - High level alerts triggered during the transaction runtime.
- KBA Challenges - Challenge question responses.

11.2 Using the Dashboard in Adaptive Risk Manager Online

The Adaptive Risk Manager Online Dashboard uses real-time data to provide a quick, overview of users and devices that have generated alerts and of all alerts by geographic location. It displays different levels of security to help you analyze online traffic, identify suspicious behavior, and design rules for fraud prevention. The dashboard also offers both total time views and trending views of performance levels.

To view the dashboard, click Dashboard on the menu bar.

The dashboard is divided into three panels:

- The performance panel on the top presents current data. It shows the performance of the traffic that is entering the system. A trending graph is shown of the different types of data based on performance.
- The summary panel in the middle presents aggregate data based on time range and different data types.
- The dashboard on the bottom presents historical data. The detailed dashboards are used for trending data over time ranges.

11.2.1 Performance

The Performance panel, at the top of the page, displays real-time interpolations that are updated at the selected rate. The numbers displayed are not totals even though they may correspond numerically to totals in many instances.

To view accurate totals and trend them over time the performance dashboard (one of the many detailed dashboards offered in the Dashboard panel) is provided in the bottom section. A good analogy to the difference between these two views is a speedometer. While driving a speedometer may display 60 m.p.h. This does not mean that during the hour you have traveled 60 miles. In reality you would have traveled 25 miles if the speed fluctuated or you stopped for gas. The top section is the speedometer and the bottom section is your actual distance traveled.

The Performance panel displays two sections: a total view on the left and a trending view on the right.

- The total view shows the statistics on the current volume or rate of logins at the present time versus the maximum.

  Max - the maximum number of logins per minute

  Current - the current number of logins per minute

- The trending view provides statistics on the selected data (how the data progresses) during the past hour.

To view the performance data:

1. Select the data type you want from the Data list.

   The data types provided are:

   - Logins per minute - Number of successful login per minute
   - KBA challenges per minute - Number of challenge question responses per minute
   - Blocked logins per minute - Number of blocked logins per minute
   - Blocked transactions per minute - Number of blocked transactions per minute
   - Transactions per minute - Number of successful transactions per minute
   - High Alerts (Logins) per minute - Number of high alerts triggered during the login runtime per minute
   - High Alert (Transactions) per minute - Number of high alerts triggered during the transaction runtime per minute.

2. To select more than one data type, control-click the types you want.

   Note: The Performance panel is intended for viewing between 1 and 3 data points at a time.

3. To change the refresh rate, click the Refresh list and then click the refresh rate you want.

Graphs are shown in different colors, which are generated on the fly, to distinguish the data schemes that are represented.

The performance panel also provides tooltips so that you can view more detailed information about the data points you are interested in. To view information using tooltips, move the mouse to the desired data point.

11.2.2 Summary

The Summary panel, in the middle of the page, displays an overview or aggregate of the selected data type for the specified range or time fame.

11.2.2.1 Data

The data types provided are:

- Login Sessions - Refers to the login sessions.
- Success Logins - Refers to successful logins.
- Temporary Allow Logins - Refers to logins that occurred while a temporary allow was active.
- Blocked Logins - Refers to logins that were blocked during the login runtime.
- High Alert (Logins) - Refers to high level alerts triggered during the login runtime.

- KBA Challenges - Refers to challenge question responses.
- Transaction Sessions - Refers to transaction id.
- Success Transactions - Refers to successful transactions.
- Blocked Transactions - Refers to transactions that were blocked during the transaction runtime.
- High Alert (Transactions) - Refers to high level alerts triggered during the transaction runtime.
- Average Rule Process Time - Average number of milliseconds for rule execution.
- Average Model Process Time - Average number of milliseconds for model execution.
- Average Runtime Process Time - Average number of milliseconds for runtime execution.

To select a data type, click the one you want from the Data list.

To select more than one data type, control-click the types you want.

11.2.2.2 Refresh

To change the refresh rate, click the Refresh list and then click the refresh rate you want.

11.2.2.3 Range

To change the range or timeframe, click the Range list and then click the range you want.

11.2.3 Dashboards

The bottom panel provides access to five different dashboard types: location, scoring, performance, device, and security. For each dashboard type you can select the type of data you want to see from a menu of data types. If you select the Location dashboard, a Country list appears that enables you to select the country you want. The left side of the dashboard panel displays a total view and the right side displays a trending view of the selected data type.

You must select a row from the table in the total view to see data in the trending view. After selecting a row or more, the trending view will show you the corresponding graph(s) of the data. Graphs are shown in different colors to distinguish the data schemes that are represented. The colors are generated on the fly; they are not predefined.

The total and trending view sections are placed side by side, and you can toggle between the views to look at the details of one more clearly. For example, you can expand the trending view section to see the entire legend instead of a portion of it.

Tooltips are particularly useful if the data points are shown closely together (packed); you can use the tooltip to gather information. For example, you may want to view data for every 1-hour sample.

The graph in the trending view adjusts accordingly based on the information being shown. The Y-coordinate will adjust depending on the highest data point. The sample will adjust based on the range. Also, whether you can choose to see data by hours, days, weeks, or months will depend on what is selected for the range.

The "Last Updated" field, which also appears in the top panel, is updated when you select a different data type.

Items in the Dashboard list are accessible based on your role. Only fraud investigators can access the Security dashboard.

To view a data type by location

1. On the Dashboard list, click Location.

   The Location dashboard appears and defaults to alerts.

2. To specify a different data type, on the Data list, click the data type you want.

   The data types provided are:

   - Alerts - provides a list of alert that have been triggered by country.
   - Actions - provides a list of actions that have been taken by country.
   - KBA Challenges - provides a list of KBA challenges that have been triggered by challenge result and country.
   - Routing Type - provides a list of a list of routing types by country.
   - Sessions - provides a list of sessions by country.
   - Temp Allow - Provides a list of temporary allows that have been made by country

3. To narrow the list to a specific country, on the Country list, click the country you want.
4. To narrow the list to a specific application ID, on the Application ID list, click the application ID you want.
5. To narrow the list to a specific timeframe, on the Ranges list, click the range you want.
6. If you selected the alerts data type, you can narrow the list further by selecting the alert level you want from the Alert Level box.
7. If you selected the alerts or temporary allow data type, you can narrow the list further by selecting the runtime you want from the Runtime list.

> **Note:** For KBA challenges from phone challenges, the country will be listed as "Data Not Available". For these records, the trending graph will not be displayed.

To view a list of scoring breakdowns

1. In the Dashboard list, click Scoring.

   The Scoring dashboard appears and defaults to risk score.

2. To narrow the list to a specific Runtime, in the Runtime list, click the Runtime you want.
3. To narrow the list to a specific timeframe, in the Ranges list, click the range you want.
4. Click Refresh.

To view a data type by performance

1. In the Dashboard list, click Performance.

The Performance dashboard appears and defaults to rules.

2. To specify a different data type, in the Data list, click the data type you want.

   The data types provided are:

   - Rules - The rules currently in the system
   - Models - The models currently in the system
   - Runtimes - The points in a session when rule is run
   - APIs - Calls into the system through the soap interface.
   - Tracker APIs - Calls into the tracker subsystem
   - Authorization APIs - Calls into the authorization subsystem
   - Common APIs - Miscellaneous calls
   - CC APIs - Calls into the customer care subsystem
   - Rules APIs - Calls to the rules processor

3. If you selected the rules or models data type, you can narrow the list further by selecting the runtime you want from the Runtimes list.
4. To narrow the list to a specific timeframe, in the Ranges list, click the range you want.
5. Click Refresh.

To view a browser and operating system data by device

1. In the Dashboard list, click Device.

   The Device dashboard appears and defaults to browser/operating system.

2. To narrow the list to a specific application ID, in the Application ID list, click the application ID you want.
3. To narrow the list to a specific timeframe, in the Ranges list, click the range you want.
4. Click Refresh.

To view a list of rule or alerts by security

1. In the Dashboard list, click Security.

   The Security dashboard appears and defaults to rules.

2. To specify a different data type, on the Data list, click the data type you want.

   The data types provided.

   - Rules
   - Alerts

3. To narrow the list to a specific application ID, on the Application ID list, click the application ID you want.
4. To narrow the list to a specific runtime, in the Runtime list, click the range you want.
5. To narrow the list to a specific timeframe, in the Ranges list, click the range you want.
6. Click Refresh.

11.3 Using the Dashboard in Adaptive Risk Manager Offline

The Adaptive Risk Manager Offline Dashboard is similar to the Adaptive Risk Manager Online Dashboard, except it uses existing real customer data from Adaptive Risk Manager Online or from a remote, custom source instead of real-time data to provide

- views of the statistics on the rate of logins
- an overview of activity
- high-level personalized views of the status of user behavior and key transactions

The Adaptive Risk Manager Offline Dashboard provides access to the "Risk Analysis" dashboard, which shows the progress of the current load or run task, and the five dashboards that Adaptive Risk Manager Online also offers.

Risk Analysis statistics are provided for

- load data: the data loaded from Adaptive Risk Manager Online or from a remote, custom source
- run data: the data that models are run against. You can run the rules against the entire database or against a subset of the database

Information is shown for the percent complete, number of records processed, number of records remaining, and estimated complete time, and so on.

12 Reporting

Adaptive Risk Manager Online is the customer care, reporting and administration application for Oracle Adaptive Access Manager. It contains a comprehensive collection of reports on:

- Users
- Locations
- Devices
- Summaries
- Security Alerts

Two types of reporting are available:

- Queries in Adaptive Risk Manager
- Oracle Identity Management Business Intelligence Publisher Reports

This chapter provides information on running queries, using Business Intelligence (BI) Publisher reports, example report scenarios, and best practices for creating reports.

12.1 Queries in Adaptive Risk Manager

This section contains the following topics:

- Running Queries in Adaptive Risk Manager
- Login Session Details
- User Details
- Device ID Details
- Location Group Details
- IP Address Details
- Statistics about Adaptive Strong Authenticator Questions

12.1.1 Running Queries in Adaptive Risk Manager

You can query the database for information on many different activities by users, locations, devices, and security alerts.

To run a query on users

1. Click Users on the Queries menu.

The Queries page on user activity appears and defaults to the report on recent logins.

2. Enter the search criteria you want and click Run Query.
3. To change the query type, click in the Query Type box and select the query type you want:
   - Recent Logins: Displays all logins within the specified time range.
   - First Logins: Displays all users first login attempt occurring during the designated date range.
   - Invalid Logins: Displays all the login attempts from invalid users occurring during the designated date range.
   - Multiple Devices: Displays all users that use multiple devices.
   - Frequent Logins: Displays all users with multiple logins within the specified time range.
   - Multiple Failures: Displays all users with multiple failures within the specified time range
   - Frequent Logins: Displays all users with multiple logins within the specified time range.
4. To view the details page for Login ID, Group ID, Device ID, Location, or IP address, click the link in appropriate column.

To run a query on locations

1. Click Location on the Queries menu.

   The Queries page on activity by location appears and defaults to the report on recent logins by location.
2. Enter the search criteria you want and click Run Query.
3. To change the query type, click in the Query Type box and select the query type you want.
   - Multiple Failures: Displays all locations with multiple failures within the specified time range.
   - Invalid Users: Displays all the locations with login attempts from invalid users occurring during the designated date range.
   - User Locations: Displays all locations a user has attempted logins from.
   - Multiple Users: Displays all locations that have multiple users.
   - Challenges: Displays success and failure rates of challenges by location.
   - Recent Logins: Displays all logins within the specified time range.
   - Users by Location: Displays all users from a given location or IP Address.
   - Frequent Logins: Displays all locations with multiple logins within the specified time range.
   - Multiple Successful Logins: Displays all locations with multiple successful logins.
   - Devices by Location: Displays all devices from a given location or IP Address.
   - Device Locations: Displays the locations for a specific device.

4. To view the details page for Login ID, Group ID, Device ID, Location, or IP address, click the link in appropriate column.
5. To schedule a report, see Scheduling a Report.

To run a query on devices

1. Click Device on the Queries menu.

   The Queries page on activity by devices appears and defaults to the report on recent logins by location.
2. Enter the search criteria you want and click Run Query.
3. To change the query type, click in the Query Type box and select the query type you want.
   - Recent Logins: Displays all logins within the specified time range.
   - Frequent Logins: Displays all devices with multiple logins within the specified time range.
   - New Devices: Displays all new device IDs created within the specified time range.
   - Multiple Users: Displays all devices that have multiple users.
   - Multiple Successful Logins: Displays all devices with multiple successful logins.
   - Multiple Failures: Displays all devices with multiple failures within the specified time range.
   - Users by Device: Displays all users from a given device.
   - Devices by Users: Displays all devices for a given User.
   - Challenges: Displays statistics about device challenged within specified time range.
   - Invalid Users: Displays all the devices with login attempts from invalid users occurring during the designated date range.
4. To view the details page Login ID, Group ID, Device ID, Location, or IP address, click the link in appropriate column.
5. To schedule a report, see Scheduling a Report.

To run a query on summaries

1. Click Summary on the Queries menu.

   The query page on summaries appears and defaults to an aggregate summary of logins by date range.
2. To change the query type, click in the Query Type box and select the query type you want.

   Logins: Displays login aggregate summary for the designated date range.

   Averages: Displays average summary for the designated date range.
3. To change the start and end date of the search, click the calendar icons and select the From and To dates you want.
4. Click Run Query.

To run a query on security

1. Click Security on the Queries menu.

   The query page on security appears and defaults to the alerts report on low, medium, and high level alerts that were generated during the specified timeframe.

2. Enter the search criteria you want and click Run Query.
3. To specify a particular location, in the Location list, click the location you want.
4. To change the alert level, in the Alert Level list, click the level you want.
5. To change the alert type, in the Alert Type list, click the type you want.
6. To find a specific alert, rule, user ID, or user name, type the search criteria in the appropriate field.
7. To change the query type, click in the Query Type box and select the query type you want.
   - Alerts: Displays all the alerts generated during the designated date range.
   - Alerts Breakdown: Displays alert breakdown summary for the designated date range.
   - Rules Breakdown: Displays rules breakdown summary for the designated date range.
   - Pre-authorization Scoring: Displays pre-authorization scoring summary for the designated date range.
   - Post-authorization Scoring: Displays post-auth scoring summary for the designated date range.
   - Score Combinations: Displays score combination summary for the designated date range.
8. To change the start and end date of the search, click the calendar icons and select the From and To dates you want.
9. To view the alert, session, or user details page, click the link you want in the report.

12.1.2 Login Session Details

The Session Details page displays an overview of the events that transpired during a particular session including the rules that ran and the rules that were triggered, the risk scores and those actions and alerts that took place.

To view the details about a login session

- On the User, Device, or Location report page, click the Session ID for the customer login you want.

  The Session Details page appears.

  In the top section of the Session Details page, Adaptive Risk Manager Online displays specific details about the session such as Session ID and User ID.

  In the bottom area, at the default state, Adaptive Risk Manager Online displays the runtimes and a master list of the actions and alerts that were triggered at those runtimes.

  To view details about the policies, click the plus sign to expand the section.

To view details about the user

- On the Session Details page, click User Name.

  The User Details page appears.

To view details about the user's primary user group

- On the Session Details page, click User Groups.

  The Group Details page appears.

  The Group Details page displays information about the primary group in which the user belongs.

To view details about the device

- On the Session Details page, click Device ID.

  The Device Details page appears.

  The top section of the Device Details page displays information about the device used to log in.

  The bottom section of the page provides access to the groups, users, actions/rule, and logins associated with that device.

12.1.3 Transaction Details

To view transactions that occurred during a session, click the Transaction Details link on the Sessions Details page. A list of transactions in chronological order is displayed. For each transaction, the Transaction ID, Transaction Type, and Time are shown.

To view details of a particular transaction, click the transaction ID. Details for that transaction will appear in the lower part of the page.

If the session has only one transaction, its details are shown by default.

If there are multiple transactions, details are shown for the last transaction on the list.

12.1.4 User Details

From the User Detail page you can view details about a user including a list of devices used by a user, the locations a user has logged in from, the alerts triggered by a user, the logins by a user, and the rules run on a user.

To view details about users

1. On the User, Device, or Location report page, click the User Name you want.

   The User Details page appears.

2. Enter the search criteria you want and click Run Query.

To view a list of devices used by this user

1. On the User Details page, click the Devices tab.

   The list of devices appears.

2. Enter the search criteria you want and click Run Query.

To view a list of locations this user has logged in from

1. On the User Details page, click the Location tab.

The list of locations appears.

2. Enter the search criteria you want and click Run Query.

To view a list of alerts triggered by a user

1. On the User Details page, click the Alerts tab.

   The list of alerts appears.

2. To search for alerts, enter the search criteria you want and then click Run Query.

To view a list of logins by this user

1. On the User Details page, click the Logins tab.

   The list of logins appears.

2. Enter the search criteria you want and click Run Query.

To view a list of rules run on this user

1. On the User Details page, click the Rules tab.

   The list of rules appears.

2. Enter the search criteria you want and click run Query.

12.1.5 Device ID Details

The Device ID page provides information about the device used to login and cross-references information about the device including groups, users, locations, alerts and rules, and logins.

To view a list of groups this device belongs to

1. On the Device Details page, click the Group tab.

   The list of groups appears.

2. Enter the search criteria you want and click Run Query.

To view a list of users that have used this device

1. On the Device Details page, click the Users tab.

   The list of users appears.

2. Enter the search criteria you want and click Run Query.

To view a list of locations from which a device has logged in

1. On the Device Details page, click the Locations tab.

   The list of locations appears.

2. Enter the search criteria you want and click Run Query.

To view a list of alerts and rules triggered by this device

1. On the Device Details page, click the Alerts/Rules tab.

   The list of alerts and rules appears.

2. Enter the search criteria you want and click Run Query.

To view a list of logins by this device

1. On the Device Details page, click the Logins tab.

   The list of logins appears.

2. Enter the search criteria you want and click Run Query.

12.1.6 Location Group Details

To view the details about a location group

1. On the User, Device, or Location report page, click the Location for the customer login you want.

   Or,

   On the Dashboard page, click the information icon next to the item you want.

   The Location Details page appears.

2. Enter the search criteria you want and click Run Query.

To view details about users from this location

1. On the Location Details page, click the Users tab.

   The list of users appears.

2. Enter the search criteria you want and click Run Query.

To view a list of devices in this location

1. On the Location Details page, click the Devices tab.

   The list of devices appears.

2. Enter the search criteria you want and click Run Query.

To view a list of alerts and rules triggered from this location

1. On the Location Details page, click the Alerts/Rules tab.

   The list of alerts and rules appears.

2. Enter the search criteria you want and click Run Query.

To view a list of logins from this location

1. On the Location Details page, click the Logins tab.

   The list of logins appears.

2. Enter the search criteria you want and click Run Query.

12.1.7 IP Address Details

To view details about the groups in which the IP is included

1. On the User, Device, or Location report page, click IP Address.

   A list of groups that include the IP is displayed.

2. Enter the search criteria you want and click Run Query.

To view details about the users associated with the IP address

1. On the IP Details page, click the Users tab.

   A list of users who have used the IP is displayed.

2. Enter the search criteria you want and click Run Query.

To view details about the devices associated with the IP address

1. On the IP Details page, click the Devices tab.

   A list of devices with the IP address is displayed.

2. Enter the search criteria you want, and click Run Query.

To view details about the alerts/rules associated with the IP address

1. On the IP Details page, click the Alerts/Rules tab.

   A list of alerts/rules associated linked to the IP is displayed.

2. Enter the search criteria you want and click Run Query.

To view details about the logins associated with the IP address

1. On the IP Details page, click the Logins tab.

   A list of logins made from the included IPs is displayed.

2. Enter the search criteria you want and click Run Query.

12.1.8 Statistics about Adaptive Strong Authenticator Questions

You can view statistics on question registration and challenge questions.

To view statistics about question registration

1. Click KBA on the Queries menu.

   The KBA Registration page appears.

   The report displays the number of users that performed each of the actions listed in the Item column and the percentage rate of successful challenges.

2. To locate the reports you want, enter the search criteria and then click Submit Query.

   - To filter the list by primary authenticator for accounts, click in the Client Type box and select the authenticator you want.
   - To Filter the list by the application ID of users, click in the Click in the Application ID box and select the ID you want.
   - To filter the list by date range, click the calendar icons and select the From and To dates.

To view statistics about challenge responses

1. Click ASA on the Queries menu.

   The ASA Challenge Response page appears.

   The report displays the number of users that performed each of the actions listed in the Item column and the percentage of customers that responded to each question.

2. To locate the reports you want, enter the search criteria and then click Submit Query.
   - To filter the list by primary authenticator for accounts, click in the Client Type box and select the authenticator you want.
   - To Filter the list by the application ID of users, click in the Click in the Application ID box and select the ID you want.
   - To filter the list by date range, click the calendar icons and select the From and To dates.

To view statistics about each challenge question

1. Click ASA on the Queries menu.

   The ASA Registration page appears.

   The report displays the number of users that performed each of the actions listed in the Item column and the percentage of challenged customers.

2. To locate the reports you want, enter the search criteria and then click Submit Query.
   - To filter the list by question category, click in the Category box and select the category you want.
   - To filter out all questions containing a specific word, enter the word in the Question Keyword field.
   - To filter the list by status, select the status you want from the status list.
   - To filter the list by date range, click the calendar icons and select the From and To dates.

12.2 Oracle Identity Management Business Intelligence Publisher Reports

Oracle Identity Management Business Intelligence (BI) Publisher Reports enables you to use Oracle BI Publisher as the reporting solution for Oracle Identity Management products including Oracle Adaptive Access Manager.

Oracle Identity Management BI Publisher Reports uses Oracle BI Publisher to query and report on information in Oracle Identity Management product databases. With minimal setup, Oracle Identity Management BI Publisher Reports provides a common method to create, manage, and deliver Oracle Identity Management reports.

The report templates included in Oracle Identity Management BI Publisher Reports are standard Oracle BI Publisher templates—though you can customize each template to change its look and feel. If schema definitions for an Oracle Identity Management product are available, you can use that information to modify and generate your own custom reports.

The *Oracle Business Intelligence Publisher Administrator's Guide* explains how to use BI Publisher to create reports for Oracle Adaptive Access Manager. You can access the *Oracle Business Intelligence Publisher Administrator's Guide* by searching for it on the Oracle Technology Network Web site.

The Oracle Business Intelligence Publisher Documentation Library is available on the Oracle Technology Network Web site. You can access the Oracle Technology Network Web site at: http://www.oracle.com/technology/index.html.

12.2.1 Configuring a Report

Oracle Adaptive Risk Manager Oracle reports are customizeable with Oracle Business Intelligence (BI) Publisher.

For information on configuring a report, see Chapter 10 of the *Oracle Business Intelligence User's Guide*. You can access the Oracle Technology Network Web site at: http://www.oracle.com/technology/index.html.

12.2.2 Creating Reports

You can create new reports for use with Oracle Adaptive Access Manager. Before creating a report, read the *Oracle Business Intelligence Publisher User's Guide* to learn how to create a report, set up a data template, export sample data, and create an RTF template using the MS Word plugin.

To create a new report:

1. Create two data models for the report.

   The model will be a File type Data Source named Properties. The Data Source will be AdminProperties, and the File Name will be properties.xml. The second will be a Data Template type Data Source.

2. On the top level of the Data Model branch in the report editor, select "Concatenated SQL Data Source" as the Main Data Set, and make sure the "Make row names unique" check box is checked.

3. To put hyperlinks in an RTF template, use the bharosa-server-url property.

   For example, if the link in FA is http://bb-beta.hyperion.com/fauio/countryDetail.do?countryId=1, then the hyperlink in the RTF template should be {/DATA/Properties/propertyList/bharosa-server-url}countryDetail.do?country={COUNTRY_ID}, assuming COUNTRY_ID is the name of the output field in the data template.

4. If a report needs additional configuration-type properties like bharosa-server-url, they can be added to the properties.xml file. Add the new properties at the same level as <bharosa-server-url>, that is, as a child of <propertyList>. You can access the new property in the RTF template as <?/DATA/Properties/propertyList/your-property-name?>.

12.2.3 Viewing a Report

To view a report, click the View link for the report.

Formats

To change the output type, select the output type from the list and select View.

- HTML
- PDF
- RTF
- Excel
- Excel2000
- PowerPoint
- MHTML

- CSV
- Data

Export

Select Export to export the report to the default application for its output type (for example: Adobe Acrobat for PDF output or Microsoft Excel for excel output).

Send

Select the Send to choose email as your delivery method. Then, enter the email addresses to send the output to.

Range

Select the range in which you want to view the data:

- Last 1 day
- Last 7 days
- Last 30 days

12.2.4 Scheduling a Report

You can schedule a report to run on a particular day and time in the future or immediately, once, daily/weekly, or monthly. If you want, you can choose to be notify by email when the report completes or fails.

To schedule a report:

1. Select the report.
2. Select the Schedule link.
3. Click Schedule a New Job.
4. Set the report parameters
   - From Date and To Date
   - Format - the output format.
   - Monitor Type
5. Set the job properties:
   - Job Name - a name for your report run.
   - Report Formatting Locale
   - Report Formatting Time Zone
   - Report Formatting Calendar
   - Public - select this check box to make this job available to all users with access to the report.
   - Save data for Republish - select this check box if you want the XML data from the report run saved.
   - Save Output - select this check box if you want the report output saved.
   - Use Unicode (UTF8)

6. In the Notification section, select when you want to be notified and if you want to use email as your notification channel. If you choose email, a field appears for you to provide an email address.
7. Enter the Time criteria.
   - Run Immediately
   - Run Once
   - Run Daily/Weekly
   - Run Monthly
8. Select Email in the Delivery section if you want the report sent by email.
9. Click Submit.

12.3 Example Report Scenarios

The following are some example reporting scenarios that may be used to investigate possible fraud. The exact reporting practices used by each institution may differ based on company policies. If a separate reporting database is not being used, great care must be taken when running reports on a live production system. All but the narrowest queries should be scheduled to run during off hours in this case.

One useful strategy is to schedule a general alert based report for each application on a nightly basis. Any suspicious activity should be further investigated using narrow queries and detail screens. Specific queries used for targeted investigation can be found in the query types menus under each of the three query families (User, Location, Device).

12.3.1 Example General Nightly Report

User/Recent logins - Schedule this report to run with the following parameters

Check Alert Level - ALERT_MEDIUM & ALERT_HIGH

Primary Group Id - The user group associated to the application

Scheduled Report

- Frequency - Day
- Range - Last 24 hours

Example Scenario 1

Nightly the User/Recent logins report is scheduled to run for the last 24 hours. One day the report shows several "Multiple failures from the device" alerts. The investigator could run a narrow query then view detail screens to gain more information. To see if the behavior that triggered the rule has been happening with a wider threshold further targeted reports could be scheduled for the next night.

12.3.1.1 User/Recent Logins

Run this narrow query with one of the specific session IDs in which the "Multiple failures from the device" alert was triggered. This session ID is the first number shown in each session listing in the general nightly report that was scheduled.

12.3.1.2 Device details

After running the narrow recent logins query the details screens associated with the login session can be viewed. These detail screens have a wealth of information collected by Adaptive Risk Manager that can be used in an investigation. For example, customers attempting logins from the suspect device can be seen on the device details screen under the users tab. If desired, action outside of Fraud Analyzer can be taken to investigate these customers for more information. For example, customers could be called to see if they have been experiencing problems accessing their account. Action from here should be guided by your institution's policies.

12.3.1.3 Device/Multiple Failures

A targeted report could be scheduled to run in response to the activity seen in the general report if a deeper look into the data is desired. Schedule this targeted report with the threshold values a bit higher than the specific rule that was triggered the previous day. The session details screen for each session ID will show what rules were triggered and there are links to the model edit screen where the exact thresholds of the rules can be seen. Any devices with exceptionally high numbers of failures should be looked into using their device details screens. Here are some example values that could be used.

Min No. Of Login Failures - 15

From and To Dates - a range corresponding to the last 48 hours

Scheduled Report

- 2 am

Example Scenario 2

Nightly the User/Recent logins report is scheduled to run for the last 24 hours. One day the report shows a "Login from restricted country" alert. The investigator could run a narrow query then view detail screens to gain more information. To see if the behavior that triggered the rule has been happening with a wider threshold further targeted reports could be scheduled for the next night.

12.3.1.4 User/Recent Logins

Run this narrow query with the specific session ID in which the "Login from restricted country" alert was triggered. This session ID is the first number shown in each session listing in the general nightly report that was scheduled.

12.3.1.5 Location details

After running the narrow recent logins query the details screens associated with the login session can be viewed. These detail screens have a wealth of information collected by Adaptive Risk Manager that can be used in an investigation. For example, customers attempting logins from the suspect countries can be seen on the location details screen under the users tab. If desired, action outside of Fraud Analyzer can be taken to investigate these customers for more information. For example, customers could be called to see if they have been accessing their accounts from outside of the USA. Action from here should be guided by your institution's policies.

12.3.1.6 Location/Users by Location

A targeted report could be scheduled to run in response to the activity seen in the general report if a deeper look into a single location is desired. Schedule this targeted report with a specific IP or geographic location. Any users found to be attempting

logins from restricted cou8ntries should be looked into. Here are some example values that could be used.

Country Name X

From and To Dates - a range corresponding to the last 48 hours

Scheduled Report

- 2 am

12.3.2 Additional Sample Analyses

Similar to the analysis processes above, other reports can be used to investigate specific situations. Here are some more examples of useful reports to run after viewing the following alerts.

- If the "Multiple Logins from IP" alert is triggered, run **Location - Multiple Users** report to see if there were any IPs recently that had a high number of users.
- If the "Multiple users are using the same device in short time frame" alert is triggered, run **Device - Multiple Users** report to see if there were any devices recently that had a high number of users with specific IP or geographic location parameters.
- If the "Login from restricted device" alert is triggered, run the **Device - Users by Device** report which will show the users that used a restricted device to login.

12.3.2.1 Here are some example values that could be used.

Specific IP or a Geographic location

From and To Dates - a range corresponding to the last 48 hours

Scheduled Report

- 2 am

12.3.2.2 Device/ Users by Device

If the "Login from restricted device" alert is seen in a nightly report this targeted report could be run the next night. This report will show the users that used a restricted device to login. Here are some example values that could be used.

Device Group - Restricted Devices

Group Id - Default user group for the application

From and To Dates - a range corresponding to the last 48 hours

Scheduled Report

- 2 am

12.4 Best Practices for Creating Reports

Customer Statistic	Reports	Directions	Notes
identify Kiosk/public machines	Device/Multiple Users	Turn up minimum number of users to an exceptional level to detect devices with extremely high numbers of users.	
How many incorrect usernames are entered per month?	User/Invalid Logins	Set min number of attempts to 1 and the time range to a month	
Identify users that use a very high number of computers to login	User/Multiple Devices	Turn up minimum number of devices to an exceptional level to detect users with high numbers of devices.	The customer profile rules could be adjusted if it is discovered that the majority of users use more than the maximum allowed devices
Identify new online users	User/First Login		
	User/Frequent Logins		
Identify the number of users having problems logging in	User/Multiple Failures	Set min number of attempts to a low number like 3 and the time range to one month	This will give a general idea of the difficulty users are having successfully logging in. However, hacker activity can skew these numbers

Hacker Issues	Reports	Notes
Brute Force		
locate possible brute force attacks	Device/Multiple Failures	Turn up minimum number of failures to an exceptional level to detect devices failing to login an abusive number of times.
	User/Multiple Failures	Turn up minimum number of failures to an exceptional level to detect users failing to login an abusive number of times.
	Location/Multiple Failures	Select a location and increase minimum number of failures to an exceptional amount.

Hacker Issues	Reports	Notes
	User/Multiple Devices	Turn up minimum number of devices to an exceptional level.
	Location/Invalid Users	Turn up minimum number of attempts to an exceptional level.

Part V

Using Adaptive Risk Manager Offline

This part provides information about creating database configurations, loading data, creating session sets, and running data for evaluation.

Part V contains the following chapter:

13

Using Adaptive Risk Manager Offline

The chapter provides information for setting up Adaptive Risk Manager Offline and on loading and running session sets—subsets of a larger body of data—for evaluation using Oracle Adaptive Access Manager Offline.

13.1 Concepts

This section provides a brief introduction to Adaptive Risk Manager Offline and contains the following sections:

What Does Adaptive Risk Manager Offline Do?

Adaptive Risk Manager Offline is an offline fraud analysis tool for evaluating existing data. It can be used in three ways:

- As a research and development tool to create and validate new rules using sample data from the production system before introducing them into an online environment
- As a standalone security tool to analyze, detect, and alert high risk situations
- As a supplemental analysis tool to aid in the tuning of rules and verification of rules behavior against real customer data without impacting customers in real-time log ins and transactions

Adaptive Risk Manager Offline Architecture

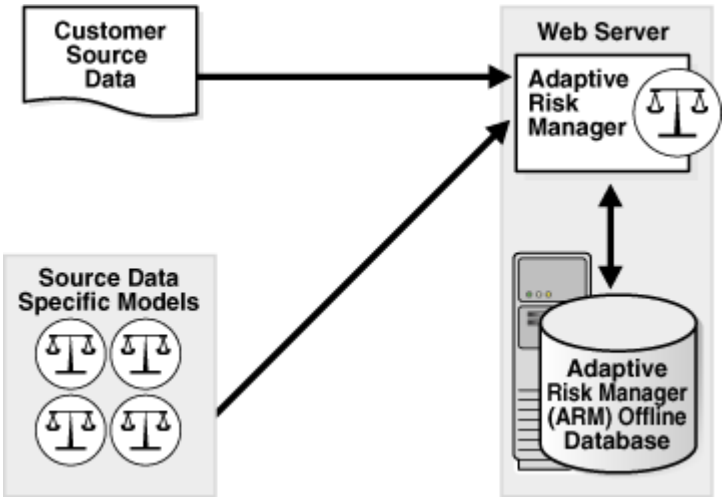
The installation of Adaptive Risk Manager Offline is similar to that of Adaptive Risk Manager Online, only Adaptive Risk Manager Offline has its own database. This additional database is the same as that of the Adaptive Risk Manager Online version.

Customer login and/or transaction data is loaded into the Adaptive Risk Manager Offline database. Data can be loaded:

- directly from Adaptive Risk Manager Online (DB Loader)
- from a temporary database (DB Loader)
- from a remote, custom source (Custom Loader)
- through a file (File-Based Loader)

Loading from a database is the standard loading process.

Adaptive Risk Manager Offline uses its Offline database, where real customer data is loaded, to perform risk analysis or conduct simulations of Adaptive Risk Manager Online.



The same models and rules as Adaptive Risk Manager Online or modified models and rules may be used to perform risk analysis.

Loaders

- DB Loader - Adaptive Risk Manager Offline, by default, is pre-configured to handle loading from a database. You will have to configure your database connection URL and so on for DB loader to access the offline data. Information about setting the URLs and other parameters is provided in Section 13.2, "Creating a New Database Configuration to Access Offline Data."

  The DB loader is preferred over the file-based and custom loaders since the DB Loader is optimized. It provides better control and is easier to use and faster:

  – for pausing and resuming

  – for working with partial data set

  Instead of using a file-based/custom loader, you may want to consider loading file or storage data into a temporary database using the standard tools and then using the temporary database to load data into the Offline database.

- Custom Loader - Custom loaders handle loading from a file or any kind of storage facility. Instead of using a custom loader, you may consider copying the data into a temporary database and using the temporary database to load the data into Adaptive Risk Manager Offline.

- File-Based Loaders - File-based loaders perform the job of taking a file and turning that into a format that you can use in Adaptive Risk Manager Offline. If a file-based loader must be used, you must first sort the file in data order. The disadvantages of the file-based loader is that Pause and Resume are slow and you will have to deal with partial session sets.

More information and guidelines for custom and file-based loaders are in Section 13.3, "Data Loaders."

Adaptive Risk Manager Offline User Flow (if using Standard Loading)

The User flow for Adaptive Risk Manager Offline using the standard loading process is shown below.

1. Install Adaptive Risk Manager Offline
2. Create and edit a DB Configuration to access offline data.
3. Create a Run Configuration with the characteristics of the run session.
4. Create Session Sets based on past dates and times.

   If you create a session set, you can choose to auto-increment the data—to pull new data periodically from the database—or pull only the data that falls within a specific date range.
5. Setting up Auto-learning
6. Load data based on a Session Set and DB Configuration.
7. Run rules against the data
   - Entire database or subset (session set)
   - Immediately or on schedule

   Alerts will be generated for suspicious activities.
8. Examine Dashboard and Reports.
9. Discover hacking attempts.
10. Create new rules and models to trap the attacks.
11. Run the old data through the new rules and models.
12. Reexamine reports to see if the new rules helped.
13. Test the rules in pre-production.
14. Implement new rules and models on Adaptive Risk Manager Online.

13.2 Creating a New Database Configuration to Access Offline Data

Source data must be loaded into the Adaptive Risk Manager Offline database so that Adaptive Risk Manager Offline can use its own database to perform risk analysis.

Instructions for creating a database configuration (setting up the parameters) for connecting to the remote database so you will be able to load or run data in the Adaptive Risk Manager Offline database is presented in this section.

If you are using a custom or file-based loader, skip this section, and go on to Section 13.3, "Data Loaders."

In creating a load configuration, you will:

- specify the characteristics of the offline load session. For example, date format, transaction size, write pool size, and so on.
- set up parameters for connecting to the remote database such as URL, password, server type (Oracle driver, SQL server driver, and so on)
- configure properties to map such fields as the table name, user Id, and browser string

13.2.1 Steps to Create the DB Configuration

To create a load configuration:

1. On the Admin menu, point to DB Configurations and then click Create Configurations.

   The Create Configurations page appears.

2. From the Configuration Type menu, select Load.

3. From the Config Name menu, select Create New Configuration.

   If you've already created the configuration, you can select from the names of existing configurations.

   The Create New Configurations page appears.

4. Enter a name for the configuration.

5. From the Status menu, select the status you want:

   Active (Enable) or Inactive (Disable)

6. Enter any appropriate notes.

7. Click Create.

   The properties panel enables you to configure and edit properties.

8. Review the list of properties and modify depending upon the location and structure of your data source and then click Save.

   Details about setting the properties are documented below.

   After creating the DB Configuration, create the Run Configuration as per the instructions in Section 13.4, "Creating a New Run Configuration."

13.2.2 Setting Properties to Load Data from an Adaptive Risk Manager Online Database

The properties labeled Remote RA DB Type, Remote RA DB Class, Remote RA DB JDBC URL, Remote RA DB User or Schema, and Remote RA DB Password will need to be changed to the values required to connect to the remote Adaptive Risk Manager database.

For example:

Edit the Remote RA DB JDBC URL and change it from `@remotehost:1521:ORCL` to your appropriate `hostname:port:SID`. For example,

```
@oaam-adm.example.com:1521:inf01
```

Change the Remote RA DB User or Schema from `brsawf` to your appropriate username. For example,

```
oaamdbuser
```

13.2.3 Setting Properties to Map the Table Name

Set the value of the property labeled Load Table Name to the name of the table containing the login data. This property value may also include a table alias, for example, `table t`. If the data is spread across multiple tables, this property can contain join criteria, for example, `table1 t1 left outer join table2 t2 on t1.id = t2.id`.

13.2.4 Setting Properties to Map Fields

Set the values of the following to the required field expressions.

- Load login time column
- Load user Id column
- Load login Id column
- Load IP column
- Load browser user agent column
- Auth status column
- Load group id column
- ClientType column
- Load secure cookie column
- Load device id column
- Load session id column
- Load expected digital cookie column

Valid field expressions include database field names (qualified with table aliases if table aliases were specified in the Load Table Name property), for example, t1.tstamp or constants, for example, null, "ra-group".

13.2.5 Setting Properties to Load Data Without Running Rules

If you want to load data without running the rules, set the Load and Run Rules property to false. If you want to run data without doing a load, create a run type DB Configuration and the property will not be available.

13.2.6 Configuring Worker/Writer Threads

While creating the loader configuration, start with 10 worker threads and watch the throughput (number of requests processed per minute) using the Dashboard.

If the throughput is not satisfactory, increase writer threads in increments of 5.

Higher number of writer threads does not necessarily result in better throughput. Adjust the number of worker threads for max throughput for the given hardware.

Check Section 13.9, "Monitoring Adaptive Risk Manager Offline" for possible worker thread starvation.

13.2.7 Setting Throttle Size

Load/ Run pauses only after buffer is flushed. When there is need for pause/resume, keep the throttle size lower. The default is 15000.

13.3 Data Loaders

This section contains information and instructions for using data loaders.

13.3.1 Quality of Input Data

If data is to be loaded into a database, make sure the data is valid as per mappings. Source data validation (basic sanity checks) is easier to perform before starting the load. It will save loading cycles and the incorrect processing of information.

Validations are:

- Check for null or empty required fields (like user name)
- Ensure that there are not too many log ins/transactions from the same user, and incorrect delimiter or escaping resulted in user id "0" being logged in more than 30% time. These kinds of errors will not necessarily result in an error, but they will slow loading process and process the data incorrectly.
- Check that the combination of fields expected to be unique and the data are unique.
- Make sure the source data does not have duplicate records/content. Duplicate records will skew the results and might raise false alerts.
- Make sure the field that identifies the request (Request Identifier) is unique.
- To avoid data truncation, make sure source data is not truncated while loading into database if the source data is loaded into database before it is fed to Oracle Adaptive Access Manager.

13.3.2 Configuring Device Data

If the source data does not have secure cookies and/or digital cookies, send constant secure cookies and/or digital cookies and turn off rotating cookies in Oracle Adaptive Access Manager.

13.3.3 Setting Properties to Load Data from a Custom Database

If you are loading from a custom database, you need to set the properties labeled Remote RA DB Type, Remote RA DB Class, Remote RA DB JDBC URL, Remote RA DB User or Schema, and Remote RA DB Password to the required to connect to the custom database.

13.4 Creating a New Run Configuration

For run, you will specify the characteristics of the offline run session: transaction size, throttle, write pool size.

You will use the run configuration when you run rules against the entire database or against a subset of the database.

To create a new run configuration

1. On the Admin menu, point to DB Configurations and then click Create Configurations.

   The Create Configurations page appears.

2. From the Configuration Type menu, select Run.
3. From the Config Name menu, select Create New Configuration.

   If you've already created the configuration, you can select from the names of existing configurations.

   The Create New Configurations page appears.

4. Enter a name for the configuration.
5. From the Status menu, select the status you want:

   Active (Enable) or Inactive (Disable)
6. Enter any appropriate notes.
7. Click Create.

   The properties panel enables you to configure and edit properties.
8. Review the list of properties at the bottom of the page and modify depending upon the location and structure of your data source.
9. Click Save.

13.5 Creating Session Sets

Transactions can be grouped into session sets, subsets of a larger body of data, and played back and studied for trends.

After the administrator has loaded the database configurations into Adaptive Risk Manager Offline, you can run the rules against the entire database or against a session set.

If you create a session set, you can choose to pull:

- new data periodically from the database (auto-increment the data)
- only the data that falls within a specific date range

13.5.1 Creating an Auto Increments Session Set

An auto increment session set pulls new data at preset intervals from Adaptive Risk Manager Online.

To create an auto increment session set:

1. On the Manage Data menu, point to Sessions Sets and then click Create Session Set.

   The Create Session Set page appears.
2. From the Set Type menu, select Auto Increment.
3. From the Set Name menu, select Create New Session Set.
4. Enter a name for the session set.
5. Enter any appropriate notes.
6. To start auto-incrementing on a specific date, click the calendar icon and select the date you want.
7. Click Create and then click Save on the next page.

13.5.2 Creating a Date Range Session Set

A date range session set pulls only the data that falls within a specific date range.

To create an date range session set:

1. On the Manage Data menu, point to Sessions Sets and then click Create Session Set.

The Create Session Set page appears.

2. From the Set Type menu, select Date Range.
3. From the Set Name menu, select Create New Session Set.
4. Enter a name for the session set.
5. Enter any appropriate notes.
6. Click the calendar icons and select the From Date and To Date.
7. Click Create and then click Save on the next page.

13.6 Enabling Adaptive Risk Manager Functionality

There are a few functions that are disabled in Offline. They can be reconfigured by adding properties to bharosa_server.properties file. Details for bharosa_server.properties are provided in the *Oracle Adaptive Access Manager Installation and Configuration Guide*.

In addition to the properties in bharosa_server.properties, you may want to turn on the following features.

13.6.1 Auto-learning

To use Auto-learning (pattern analysis):

1. Import default entities.
2. Enable Auto-learning properties

```
vcrypt.tracker.autolearning.enabled=true
vcrypt.tracker.autolearning.use.auth.status.for.analysis=true
vcrypt.tracker.autolearning.use.tran.status.for.analysis=true
```

3. Define and enable patterns.
4. Perform load and the run at the same time.

   You cannot perform the load and then the run if you want Auto-learning.

Refer to Chapter 8, "Auto-learning and Patterns" for detailed information about Auto-learning and pattern creation.

13.6.2 Rule Logging

Rule Logging for detailed information can be turned on by setting:

```
vcrypt.tracker.rules.trace.policySet=true
vcrypt.tracker.rules.trace.policySet.min.ms=100
```

13.6.3 Configurable Actions

Configurable actions can be enabled by setting:

```
dynamicactions.enabled=true
```

For information on configuring a Configurable Action, refer to Chapter 5, "Configurable Actions."

13.7 Loading and Running Data for Offline Evaluation

This section contains instructions for

- Loading Data
- Running Data

13.7.1 Loading Data

When you load a session set you specify:

- the database configuration you want to use
- the session set-or subset of that database-you want to run
- the interval type if you're using an auto-increment session set
- to load Immediately or to load by a schedule

To load data:

1. On the Manage Data menu, point to Run/Load and then click Load Data.

   The Load Data page appears.

2. Enter a name for the session data that is being loaded.
3. From the Config menu, select the load configuration that has been created for this load.

   For information on the load database configurations, refer to Section 13.2, "Creating a New Database Configuration to Access Offline Data."
4. From the Session Sets menu, select the session set you want.
5. Enter any appropriate notes.
6. If you want to load the data immediately, click Load. If you want to schedule the load instead, skip this step and continue on to the next step.
7. To schedule load data:

   a. select the Interval Type

      The Interval Type is the frequency of the schedule. You can choose Daily, Hourly, Monthly, None, or Weekly.

   b. select the Suspend Time, if required

      Suspend Time is the number of hours the task should be allowed to run before it is automatically stopped.

   c. enter a Begin Time

      Begin Time is the start date for the schedule. For example, 06/01/08 02:00 hours.

   d. enter an End Time

      End Time is the end date for the schedule. For example, 07/31/08 23:59 hours.

   e. enter an Interval Value

      Enter a valid positive numeric value. It cannot be zero. This is the time-off value in between schedules. For example, in an hourly schedule where the interval value is 2, if the current schedule runs at 06:00 hours, after an interval of 2 hours, the next schedule will begin (08:00 hours).

Then, click Schedule.

13.7.2 Running Data

When you run data you specify:

- the database configuration you want the data to come from
- the session set (the subset of the data) that you have predefine and now want to run

  For example, you may have created a session set that specifies a date range during which you observed suspicious activity.
- to run the data Immediately or by a schedule

To run data:

1. On the Manage Data menu, point to Run/Load and then click Run Data.

   The Run Data page appears.
2. Enter a name for the data you want to run.
3. From the Config menu, select the run configuration that has been created to run data.

   For information on run database configurations, refer to Section 13.2, "Creating a New Database Configuration to Access Offline Data."
4. From the Session Sets menu, select the session set you want.
5. Enter any appropriate notes.
6. If you want to run the data immediately, click Run. If f you want to schedule the run instead, skip this step and continue on to the next step.
7. To schedule run data:
   a. select the Interval Type

      The Interval Type is the frequency of the schedule. You can choose Daily, Hourly, Monthly, None, or Weekly.

   b. select the Suspend Time, if required

      Suspend Time is the number of hours the task should be allowed to run before it is automatically stopped.

   c. enter a Begin Time

      Begin Time is the start date for the schedule. For example, 06/01/08 02:00 hours.

   d. enter an End Time

      End Time is the end date for the schedule. For example, 07/31/08 23:59 hours.

   e. enter an Interval Value

      Enter a valid positive numeric value. It cannot be zero. This is the time-off value in between schedules. For example, in an hourly schedule where the interval value is 2, if the current schedule runs at 06:00 hours, after an interval of 2 hours, the next schedule will begin (08:00 hours).

   Then, click Schedule.

13.7.3 Re-loading and Re-running the Same Data

Once records have been loaded from a data source, the system will not allow you to go back and load earlier records from that same data source. If you need those records, you must create a new identical DB Config, and use that to load the earlier records. Be sure that the dates on your session set do not overlap with existing records, or you will have duplicate records.

13.7.4 Re-running the Same Session Set

If you realize that your rules are not functioning as expected, you can rerun the same session set. You will not have to perform any purging procedures on the alerts that were generated. They will be purged automatically when the same session set is run.

13.8 Controlling Adaptive Risk Manager Offline

This section contains information on stopping and pausing Adaptive Risk Manager Offline.

13.8.1 Stop

Use Stop if there is need to stop the Load/Run process immediately. Stop will flush requests in the queue and stop the process. "Pause" is preferred over "Stop".

The Resume option is not available for a stopped process. A new session set has to be created to resume the process.

13.8.2 Pause

Use Pause to continue processing requests in the queue and then stop. Pause will stop reading source data but will continue to process the requests in the queue.

13.9 Monitoring Adaptive Risk Manager Offline

This section describes how to monitor Adaptive Risk Manager Offline using the Dashboard and Server Logs.

13.9.1 Using Dashboard to Monitor the Loader Process

Use the Adaptive Risk Manager Offline Dashboard to view the statistics on the rate of log ins; the data loaded from Adaptive Risk Manager Online (session set) or from a remote, custom source (load); the data that models are run against (run). Refer to Chapter 11, "Using the Dashboard."

Please note that in Offline, the reports on the dashboard are based on the execution time rather than the login time (as in Online).

Use the following sections of the Dashboard to monitor the loader process:

1. The performance panel on the top gives the throughput in terms of log ins per minute, transactions loaded per minute, and so on. A trending graph is shown of the different types of data based on performance so that loader trends can be monitored.
2. The dashboard on the bottom presents historical data. Select Performance from the Dashboard list. Performance can be monitored in terms of average response time of APIs, Rules, and so on. Trend graph are available for the selection.

13.9.2 Oracle Adaptive Access Manager Server Logs

For every 1000 requests processed, the loader process prints the time taken to process those 1000 requests. These logs provide a good indication of throughput.

13.9.3 More Logs

Make sure you have the following properties set:

```
bharosa.db.query.performance.warning.print.stack=false
bharosa.db.query.performance.warning.threshold.ms=200
```

The server writes SQLs that took more than 200ms to execute to log file.

Random SQLs in logs are fine, considering the load being handled. However, higher number of SQLs indicate possible improvements in DB or Network areas.

13.9.4 Database Tuning

You can monitor and tune the performance of the database using tools like Oracle Enterprise Manager.

13.10 Examining Reports for Verification

Many reports are available in Oracle Adaptive Access Manager that makes it easier to monitors Adaptive Risk Manager Offline to identify fraudulent attempts and opportunities for optimization and report fraudulent attempts. For more information on reports, refer to Chapter 12, "Reporting."

13.11 Creating New Models and Rules

After discovering trends and suspicious activity, you can start creating new rules and models to capture these attacks.

1. Create new rules and models to trap the attacks.
2. Run the old data (predictable data) through the new rules and models to ensure they are functioning as expected.
3. Reexamine reports to see if the new rules helped.
4. When you are satisfied that the model is functioning as expected, migrate the model in pre-production where performance testing can be run.

   This is an important step since the new rule template and/or model can potentially have a big performance impact. For example, if you define a new model to check that a user was not using an email address that had been used before (ever). If you have over 1 billion records in your database, performing that check against all the records for every transaction will have a great impact on performance. Therefore, testing the model under load is important.
5. Only when you are satisfied that your new rule/model is functioning as expected and does not adversely affect performance should it be implemented on Adaptive Risk Manager Online.

13.12 Viewing Configurations, Loads, Runs, and Tasks

This section contains the following topics:

- Viewing a List of Database Configurations
- Viewing a List of Session Sets
- Viewing a List of Loads
- Viewing a List of Scheduled Tasks
- Viewing a List of Runs

In 10.1.4.5.2, a new Scheduler user interface for viewing internal system tasks is present for both Adaptive Risk Manager Online and Offline. In Offline mode, the new user interface is in addition to the standard Adaptive Risk Analyzer Offline Scheduler for viewing loads and run in Offline. For debugging purposes, this new Scheduler user interface is not used for scheduling tasks.

13.12.1 Viewing a List of Database Configurations

To view of list of database configurations:

1. On the Admin menu, point to DB Configurations and then click List Configurations.

   The List Configurations page appears.
2. To quickly find the configuration you want, enter the name of the configuration.
3. To filter the list by configuration type, from the Type menu, select the type you want.
4. To filter the list by status, from the Status menu, select the status you want.
5. Press Submit Query.
6. Click the configuration you want.

   The Create Configurations page for that configuration appears.

13.12.2 Viewing a List of Session Sets

To view a list of all session sets:

1. On the Manage Data menu, point to Sessions Sets and then click List Session Sets.

   The List Session Sets page appears.
2. To quickly find the session set you want, enter the name.
3. Click Submit Query.
4. In the list of session set, click the name of the session set you want.

   The Create Session Sets page appears.
5. To delete a session set, select the session set you want and click Delete.

13.12.3 Viewing a List of Loads

You can view a list of session sets that have been loaded into Adaptive Risk Manager Offline.

To view a list of loads:

1. On the Manage Data menu, point to Run/Load and then click List Loads.

   The List Loads page appears.

2. To quickly find the load you want, enter the name.
3. To filter the list by status, from the Status menu, select the status you want.
4. To narrow the list by date range, click the calendar icons and select the From and To dates you want.
5. Click Submit Query.

   The List Load page appears.
6. To delete a load, select the load you want and click Delete.
7. If you want to view details about the load, click the load you want.

   A screen with the load details appears.

   Use the pause/resume button if you want to pause the load and resume it later.

13.12.4 Viewing a List of Scheduled Tasks

To view a list of scheduled tasks:

1. On the Manage Data menu, point to Run/Load and then click List Schedulers.

   The List Schedulers page appears.
2. Specify the search criteria:
   - Schedule Name
   - Schedule Type
   - Interval Type
   - Status
   - Date range
3. Click Submit Query.

   The List Scheduler page appears.
4. To delete a scheduler, select the scheduler you want and click Delete.
5. If you want to view information about the scheduler, click the scheduler you want.

13.12.5 Viewing a List of Runs

You can view a list of runs that have been loaded into Adaptive Risk Manager Offline.

To view a list of runs:

1. On the Manage Data menu, point to Run/Load and then click List Runs.

   The List Runs page appears.
2. To quickly find the run you want, enter the name.
3. To filter the list by status, from the Status menu, select the status you want.
4. To narrow the list by date range, click the calendar icons and select the From and To dates you want.
5. Click Submit Query.

   The List Run page appears.
6. To delete a run, select the run you want and click Delete.

You cannot delete a run when run is in progress or when logs are associated with it. In those cases, you can stop or pause the run.

7. If you want to view details about the run, click the run you want.

   A screen with the run details appears.

   Use the pause/resume button if you want to pause the run and resume it later.

13.13 Troubleshooting

This section provides information on how to troubleshoot problems that you might encounter when using Adaptive Risk Manager Offline.

13.13.1 During Load: An Out of Memory Error Occurs When Loading Data From a Microsoft SQL Server

Make sure the connection string specified for Remote RA DB JDBC URL in your DB Config contains the parameter, "selectMethod=cursor", as shown in the example below:

```
jdbc:sqlserver://localhost:1433;databaseName=oaam_offline;selectMethod=cursor
```

13.13.2 During Load: No Records are Loaded and the Status is Complete

If you encounter situations where no records are loaded and the Status is Complete, the following steps may help when trying to resolve the issues:

1. Check the JDBC parameters in your DB Config for correct database configuration.
2. Ensure begin and end dates in session set definition are set per your needs.
3. Check logs for errors.

13.13.3 During Load: No Records are Loaded and the Status is Error

Follow the steps below to gather information if no records are loaded and the Status is Error.

1. Check the DB Config, paying special attention to the JDBC URL, user name, and password.
2. Check logs for errors.

Part VI

Troubleshooting

This part provides information for troubleshooting symptoms and gives solutions to the difficulties you may experience.

Part VI contains the following chapter:

- Chapter 14, "Troubleshooting"

14

Troubleshooting

This chapter describes common troubleshooting issues and tips to resolve them.

14.1 Adaptive Risk Manager

Common issues in Adaptive Risk Manager are documented in this section.

14.1.1 Oracle Adaptive Access Manager is Slow to Respond

Oracle Adaptive Access Manager is slow to respond; and diagnostics, logs, and errors—such as "hogging thread counts and a large number of SQL*net and RX errors—indicate a network issue.

If you are experiencing a network performance issue, monitor your network interface using a network utility like Ethtool (for Linux) to help you analyze your network bottleneck.

14.1.2 SOAP Service Calls Throws Exceptions

Check if the remote calls do have DNS lookup or network connectivity. Check the DNS lookup capabilities. Using IP, instead of name may be faster.

Make sure soap time out is not set to too low. Parameter "vcrypt.soap.call.timeout" affects the timeout and default is set to 3000 (3 secs)

14.1.3 Adaptive Risk Manager Online Is Not Accessible

Check the port on which the application server is active and serving the Adaptive Risk Manager Online application.

Make sure DNS entry is correct and/or IP Address is accessible.

14.1.4 Rule Execution Logs Do Not Appear in Session Details

Rule execution logs are written asynchronously and may not be available immediately. Check back later to see if they are available.

14.1.5 Unable to Login Into Adaptive Risk Manager

Check that the user id has access and is a member of the predefined roles. The roles are defined in the application server for Adaptive Risk Manager.

14.1.6 Adaptive Risk Manager Online Is Accessible But Queries Return Database Errors

Ensure correct database access credentials are used in the sessions.xml. If data source is used, make sure data source is configured correctly.

Check that the TCP/IP port specified on the database server for database access is correct and the database server is listening on the port.

14.1.7 Adaptive Risk Manager Online Application Throws Timeout Errors

Check the timeout settings for the application server container.

14.1.8 Unable To See All The Menus In Adaptive Risk Manager Online

Check that the user ID is a member of the predefined roles, which were defined in the application server for Adaptive Risk Manager.

14.1.9 Rule Conditions Import Causes weblogic.jdbc.wrapper.Clob_oracle_sql_CLOB Exception

Problem: While importing the rule conditions using Oracle XE configured through JNDI, a weblogic.jdbc.wrapper.Clob_oracle_sql_CLOB exception occurs. The trace references Oracle8Platform.writeLOB.

Solution: Change the platform class in sessions.xml file to com.bharosa.common.db.wldbutil.Oracle10PlatformLOBUtil and restart WebLogic.

14.1.10 Import Fails in Adaptive Risk Manager Deployed in WebLogic

Problem: Adaptive Risk Manager is deployed in WebLogic server. Import fails with following error:

```
weblogic.jdbc.wrapper.Clob_weblogic_jdbc_base_BaseClob cannot be cast to
oracle.sql.CLOB
```

Solution: There is a known issue with WebLogic JNDI for handling CLOB. The current recommended workaround is to change the platform class in sessions.xml file to the one provided in the Adaptive Risk Manager distribution. Please refer "Configuring Database Connectivity" in the *Oracle Adaptive Access Manager Installation and Configuration Guide.*

14.1.11 Unable To Reset All User Information From Adaptive Risk Manager Online Customer Care

Check that the user id accessing Adaptive Risk Manager Online customer care is a member of the predefined roles, which were defined in the application server for Adaptive Risk Manager. Refer to "Adaptive Risk Manager User Groups" in the *Oracle Adaptive Access Manager Installation and Configuration Guide.*

14.1.12 Adaptive Risk Manager Offline Application Server Fails with OutOfMemory Error During Data Load

The Adaptive Risk Manager Offline application server fails with an OutOfMemory error during data load; the environment uses a SQL Server database.

To load login data from a SQL Server database, the JDBC connection string should be updated to include "selectMethod=cursor".

1. On the Admin menu, point to DB Configurations and then click List Configurations.
2. In the Properties tab of your DB Configuration, update "Remote RA DB JDBC URL" to include "selectMethod=cursor", as shown in the example below:

```
jdbc:sqlserver://localhost:1433;databaseName=oaam_offline;selectMethod=cursor
```

14.1.13 Encounter Errors While Trying To Connect To Oracle Database

If you are getting errors while trying to connect to your Oracle database, check the tns listener status.

If the tns listener is not running, start it by issuing the command:

```
lsnrctl start
```

14.2 Adaptive Strong Authenticator

Common issues in Adaptive Strong Authenticator are documented below.

14.2.1 Server, URL, and Port Problems

A large majority of potential problems related to the Adaptive Risk Manager Online system are due to incorrect settings within client-specific properties files.

When troubleshooting a problem relating to an Adaptive Risk Manager Online installation, ensure that the following two general problems have been addressed:

- Check that the port settings are correct.
- Check the URL to the Web services.

14.2.2 Adaptive Strong Authenticator Key Pad Troubleshooting

KeyPad does not display.

- Check the property:

```
bharosa.authentipad.image.url=kbimage?action=kbimage&
```

- Make certain that the client application is pointing to the correct server application.

Buttons stop jittering.

- Someone has changed the keypad settings. Check with your server personnel regarding property modifications they may have made.

Same image displayed to all users.

- Check the properties file to make sure that the backgrounds directory setting is correct.

No image displayed in pad background.

- User may have images disabled in the browser.
- Users image may have been deleted from the backgrounds directory.

- Check the properties file to make sure that the backgrounds directory setting is correct.
- Check that Adaptive Risk Manager Online is configured to assign images for personalization.

14.2.3 Change Password Feature Does Not Work

Oracle Adaptive Access Manager must be integrated with another application in order for the change password feature to work, as Oracle Adaptive Access Manager does not store user passwords. For this reason, when change password is attempted in standalone "test" mode there is no password to update.

14.2.4 Authorization Failure for SOAP Request by Adaptive Strong Authenticator

If you are unable to access Adaptive Strong Authenticator and an "Authorization Failure" error appears in your client log file, refer to "Configuring SOAP/Web Services Access" in the *Oracle Adaptive Access Manager Installation and Configuration Guide* for information on setting up SOAP/Web services access.

Part VII

Appendices

This part provides reference information.

Part VII contains the following appendixes:

- Conditions Reference
- Oracle Adaptive Access Manager Reports
- Universal Installation Option Actions
- Account Statuses
- Authentication Statuses

A

Conditions Reference

This appendix provides information about the conditions available standard on Oracle Adaptive Access Manager.

Condition Name	Condition Description
Always On - User	This rule always gets processed
Device: Browser header substring	Checks whether the supplied string exists as a substring in the browsers header information
Device: Device first time for user	If this device is used for the first time by this user
Device: Device in group	Check to see if this device is in group
Device: Excessive use	Device is excessively used but not used before
Device: Is registered	Check to see if the user has registered this device
Device: Login count	Check unique user count using this device in past x seconds
Device: Timed not status	Maximum login attempts for all but the given status within the given time period
Device: Used count for User	Device used count
Device: Velocity from last login	Triggers when miles per hour is more than specified value
Device Id: Cookie state	check the cookie state for the given device and user
Device Id: Cookies Match	Tracker Node Matches for both cookies
Device Id: Header data match	Determines if header data is match
Device Id: Header data match percentage	Determines if header data match percentage is within specified range
Device Id: Header data present	Determines if header data is present
Device Id: Http Header data Browser match	Determines if Browser is matched based on http header data
Device Id: Http Header data Browser upgrade	Determines if Browser is upgraded based on http header data
Device Id: Http Header data OS match	Determines if operating system match based on http header data
Device Id: Http Header data OS upgrade	Determines if operating system is upgraded based on http header data. Check is based on versions
Device Id: Is Cookie disabled	Determines if cookie is disabled for the user based on history
Device Id: Is Cookie empty	Determines if cookie value is empty or not empty. Validation check is not included
Device Id: Is Cookie from same device	Determines if the http and flash cookies are from same device. Automatically checks old nodes, if current node is not found

Condition Name	Condition Description
Device Id: Is Cookie Old	Determines if the cookie sent is from old cookie
Device Id: Is Cookie Valid	Determines if there is a valid node for given cookie value
Device Id: known header data match percentage	Determines if known header data match percentage is within specified range
Device Id: User ASN first time	This checks to see if the user has used this ASN successfully previously
Device Id: User Carrier first time	This checks to see if the user has used this Carrier successfully previously
Device Id: User City first time	This checks to see if the user has used this City successfully previously
Device Id: User Country first time	This checks to see if the user has used this Country successfully previously
Device Id: User IP first time	This checks to see if the user has used this IP successfully previously
Device Id: User ISP first time	This checks to see if the user has used this ISP successfully previously
Device Id: User State first time	This checks to see if the user has used this State successfully previously
Device Id: User used this finger print	This checks to see if the user has used this finger print previously
ENTITY: Entity is member of pattern bucket for first time in certain time period	Condition to check if this Entity is member of pattern bucket for first time in certain time period
ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture	Check to see if this Entity has been member of this pattern bucket based on percent basis, taking into account all other entities
ENTITY: Entity is member of pattern less than some percent times	Check to see if this Entity has been member of this pattern Condition based on percent basis
ENTITY: Entity is member of pattern N times	Check to see if this Entity has been member of this pattern Condition
ENTITY: Entity is member of bucket N times in a given time period	Condition to check if this Entity is member of bucket number of times in given time period.
Location: ASN in group	Check to see if the ASN for the current IP address is (or is not) in the ASN group
Location: Domain in group	Check to see if the Second Level Domain is in the group
Location: In carrier group	If the IP is in the given carrier group
Location: In City group	If the IP is in the given city group
Location: In Country group	If the IP is in the given country group
Location: IP Conn Speed in group	Check to see if the IP Connection Speed is in the group
Location: IP Conn Type in group	Check to see if the IP Connection Type is in the group
Location: IP connection type	Connection type for the IP. It could be DSL, Cable, ISDN, Dialup, Fixed Wireless, Mobile Wireless, Satellite, Frame Relay, T1/T3, OCx, and so on.
Location: IP Excessive use	IP is excessively used but not used before
Location: IP in group	If the IP is in the IP group
LOCATION: IP is AOL	Check to see if the IP is from AOL Proxy

Condition Name	Condition Description
Location: IP line speed type	Connection line speed type for the IP. This is categorized into High, Medium, Low or Unknown
LOCATION: IP Max logins	Maximum number of log ins using the current IP address within the given time duration
Location: IP Max Users	Maximum number of users using the current IP address within the given time duration
Location: IP Multiple Devices	Maximum number of devices from IP address within the given time duration
Location: IP routing type	Routing type for the IP. It could be fixed/static, anonymizer, AOL, POP, Super POP, Satellite, Cache Proxy, International Proxy, Regional Proxy, Mobile Gateway or Unknown
Location: IP Routing Type in group	Check to see if the IP Routing Type is in the group
Location: IP type	IP is valid, unknown or private.
Location: Is IP from AOL	Check to see if the IP is from AOL proxy
Location: ISP in group	Check to see if the ISP for the current IP address is (or is not) in the ISP group
Location: Timed not status	Maximum login attempts for all but the given status within the given time period
Location: Top Level Domain in group	Check to see if the Top Level Domain is in the group
Session: Check param value	Check to see if specified parameter value is more than specified value
Session: Check param value for regex	Check to see if specified parameter value matches regular expression
Session: Check param value in group	Check to see if specified parameter value is in group
Session: Check string param value	Check to compare string value
Session: Check two string param value	Check to compare two parameters string value
Session: Compare two parameter values	Compare two parameter values
Session: Compare with current date time	Compare specified parameter value with current time
Session: IP Changed	IP Address is changed since transaction is started
System - Check Boolean Property	Check system property
System - Check Int Property	Check system property
System - Check Request Date	Check request Date
System - Check String Property	Check system property
System - Evaluate Model	Process the model as rule and evaluate results
TRANSACTION: Check Current Transaction Using Filter	Check to see if the current transaction matches ALL the conditions specified. Up to 6 conditions can be specified.
TRANSACTION: Check Transaction Aggregrate And Count Using Filter	Check the aggregrate of a numeric field and transaction count. You can specify the criteria for the transaction to be counted using the filter conditions (up to 6 conditions) and also the other parameters, like duration, to be considered and the transaction status to consider, and so on.
TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions	Check to see if the count of a transaction entity or entity/data element with a given count where transactions matches ALL the conditions specified. Up to 6 conditions can be specified.

Condition Name	Condition Description
TRANSACTION: Check if consecutive Transactions in given duration satisfy the filter conditions	Check if consecutive transactions in a given duration satisfy the specified filter conditions
TRANSACTION: Compare Transaction Aggregrates (Sum/Avg/Min/Max) across two different durations	Compare transactions aggregrates across two different durations
TRANSACTION: Compare Transaction counts across two different durations	Compare transactions counts across two different durations
TRANSACTION: Compare Transaction Entity/Element counts across two different durations	Compare transaction entity/element counts across two different durations
TRANSACTION: Compare Transaction Entity Or Element Counts Across Durations	Compare transaction entity/element counts of two different durations
User: Account Status	Account status of the user
User: Action Count	Checks action counter for the given action
User: Action Count Timed	Checks to see if the given action count is more than specified count. If runtime is not specified, action is checked in all runtimes
User: Action Timed	Maximum number of actions in the past x seconds
User: ASN first time for user	Is the user using this ASN for the first time
User: Auth Image Assigned	Check to see if auth image is assigned to user
User: Authentication Mode	Check user authentication mode
User: Challenge Channel Failure	If a user has a failure counter value over a specified value from specific channel
User: Challenge Failure	If a user has a failure counter value over a specified value for more than a specific time
User: Challenge Maximum Failures	Check to see if user failed to answer challenge question for specified number of times
User: Challenge Questions Failure	Checks to see how many questions have failures
User: Challenge timed	Check to see if user answered challenge question successfully in last n days
User: Check Last Session Action	Checks to see if the given action is in last session. If runtime is not specified, action is checked in all runtimes of that session
User: Check login count	Check user login count within specified duration
USER: Check User Data	Checks User Data for the given key
User: City first time for user	Is the user using this City for the first time
User: Client And Status	Account status of the user
User: Country failure count for user	Check failure count for the user from the given country
User: Country first time for user	Is the user using this Country for the first time
User: Devices	Number of devices tried in given time
User: Distance from last successful login	Distance from last successful login within specified time
User: Distance from last successful login within limits	Check to see if distance from last successful login within specified time is within in limits
User: Image Status	Image status of the user
User: In Group	If the user is in the given group

Condition Name	Condition Description
User: IP carrier first time for user	Is the user using this IP carrier for the first time
User: Is last IP match with current IP	Checks to see if user login IP address matches with that of previous login
User: Is User Agent Match	Checks to see if user agent matches with that of previous login from same device
User: Last login	Last login within specified time
User: Location Used Timed	If user used this location within the given time period
User: Login first time for user	Checks to see if user is logging in for the first time
User: Login In group	If the user login is in the given group
User: Max Cities	Number of cities within the given time period
User: Max Countries	Number of countries within the given time period
User: Max IPs Timed	Max number of IPs within the given time period
User: Max Locations Timed	Max number of locations within the given time period
User: Max States	Number of states within the given time period
User: Multiple failures	User failed multiple times
User: Phrase Status	Phrase status of the user
User: Preferences Configured	Check to see if the user preferences are set
User: Question Status	Question status of the user
User: Runtime score	Checks to see if the score is within limits
User: Stale session	Checks to see if there is newer login after current login session is established.
User: State first time for user	Is the user using this State for the first time
User: Status Count Timed	User attempted multiple log ins in specified time
User: User Agent Percentage Match	Checks to see if user agent percentage match is above specified percentage. Compares with UAS of previous login from same device
User: User Group in Group	If the user group is in the given group
User: User is member of pattern N times	Check to see if this user has been member of this pattern Condition
User: Velocity from last successful login	Velocity from last successful login

A.1 Descriptions

Descriptions for a few of the conditions are provided below.

A.1.1 DEVICE Conditions

A.1.1.1 DEVICE: Browser header substring

Condition	DEVICE: Browser header substring
Description	Checks whether the supplied string exists as a substring in the browser's header information. String comparison is performed by ignoring the case (upper- or lowercase) of the strings.
Pre-Requisites	
Assumptions	You should have this rule configured through a model.
Available since version	Pre-10.1.4.5
Runtimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
subString	Substring which is to be checked with the string present in the browser.		Yes

Possible User Scenarios

This condition can be potentially used to determine if the user is coming in from a particular version of a browser that is prone to security problems.

A.1.1.2 DEVICE: Device firsttime for user

Condition	DEVICE: Device firsttime for user
Description	Checks if user is using this device for the first time ever. Please note that device is the combination of the physical device and the browser in most of the test scenarios. Please check the recent logins page to determine the device id associated with the login sessions to verify the rule. The user's current (session) device is also counted as when found to be used for the first time.
Pre-Requisites	You should have this rule configured through a model.
Assumptions	
Available since version	Pre-10.1.4.5
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
is	Boolean that checks if the condition should return true or false if the user is using this device for the first time	true (default) or false	Cannot be Null.

Possible User Scenarios

This condition can be potentially used to determine if the user is coming in from a different device or different devices and then challenge him if it is the case.

A.1.1.3 DEVICE: In Group

Condition	DEVICE: In Group
Description	Checks to see if this device is in the specified list.
Pre-Requisites	There should be a list defined already which has devices (ids) as members. You should have this rule configured through a model.
Assumptions	
Available since version	10.1.4.5
Runtimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
isInList	This is a boolean parameter that defines a default return value if the device is in the list.	True / [False]	Yes.
listId	This is the list of ids of a list of devices. The model-rule interface will show you a menu of the possible lists of device lists. Please use the group editor in Adaptive Risk Manager to edit the device list.		Yes

Possible User Scenarios

This condition can be potentially used to determine if the device of the current activity belongs to a particular list of devices. For example, you may have certain devices—those that can be deemed as compromised—and you may want to block users coming in from the device or you may not want the users to perform certain activities if they are coming in from a device that is a kiosk etc.

A.1.1.4 DEVICE: Excessive Use

Condition	DEVICE: Excessive Use
Description	Checks to see if this device is used excessively. Basically, checks if a device was not active (not used) for a number of days and suddenly a large number of users is coming in from the same device in a short period of time (in a few hours). This condition can be potentially used to track the compromised device of some automated programs that obtained access to the code and then tries to login a number of users from there.
Pre-Requisites	You should have this rule configured through a model.
Assumptions	
Available since version	10.1.4.5
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
userCount	Number of users coming in from a single device in a short period of time.	positive integers	No

Parameter	Description	Possible Values	Can be Null?
withInHours	This parameter defines the short period of time in which we have to find the excessive use.	positive integer	No
notInDays	This is the parameter that describes how many days the device was not in use.	positive integer	No

Possible User Scenarios

This condition can be potentially used to determine if the device of the current activity is compromised. For example, you might have certain devices—those which can be deemed as compromised—and you may want to block users coming in from there. This could be, for example, somebody hacking into a bank computer and then tries to perform various activities. Typically, you would not have activity coming in from that computer for several days.

A.1.1.5 DEVICE: Is registered

Condition	DEVICE: Is registered
Description	Condition checks if the device from where user is coming in is registered for the user.
Pre-Requisites	You should have this rule configured through a model.
Assumptions	
Available since version	10.1.4.5
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
is	Boolean parameter to decide if the default return value should be true or false if the device is registered.	[True] / False	Yes

Possible User Scenarios

This condition can be used to identify if the user is coming in from a device that he has not registered before. This can basically prevent a fraud where users login information is stolen and the thief tries to login this user from some another otherwise safe location.

A.1.1.6 DEVICE: User count

Condition	DEVICE: User count
Description	Check to see if this device is used by a number of unique users in the last few seconds. This can potentially be fraud since if this condition is true then it will be potentially a compromised device or compromised login information for number of users.
Pre-Requisites	You should have this rule configured through a model.

Condition	DEVICE: User count
Assumptions	
Available since version	10.1.4.5
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
numberOfUsers	Number of users coming in from the same device in a short period of time.	positive integers	No
withinSeconds	This parameter defines the short period of time in which the numbers user try to login into the system using that device.	positive integer	No

Possible User Scenarios

This condition can be potentially used to determine if the device of the current activity is compromised. This could also mean that somebody stole login information for a number of users and then sat down to ruin there accounts. This will result in a lot of users coming in from same device in an interval of a few seconds.

A.1.1.7 DEVICE: Timed not status

Condition	DEVICE: Timed not status
Description	This condition counts the attempts by users from the same device (the device from which this attempt is coming in) in the last few seconds whose authentication status is not the one given in the condition. If this count exceeds the count configured in the condition, then this condition evaluates to true.
Pre-Requisites	You should have this rule configured through a model.
Assumptions	
Available since version	10.1.4.5
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
status	We want to count the attempts with the status that is not equal to this status.	auth.status.enum (auth.status.enum.success is the default)	No
withinSeconds	This parameter defines the short period of time in which the number of login attempts into the system using that device are to be counted.	positive integer	No
attempts	Max number of attempts that we want to watch for. If the attempt count in the ARM exceeds this number then condition will evaluate to true.	positive integer	No

Possible User Scenarios

This condition can be potentially used to determine if the device of the current activity is compromised. The possibility of fraud that can be detected here is someone (or a automated program) is using the same device to make login attempts and they are either failing or passing based on what data the thieves have stolen. Or may be some program is trying to break the password for user in an automated fashion. In these cases you would see repeated failed login attempt from the same device in a short amount of time.

A.1.1.8 DEVICE: Used count for User

Condition	DEVICE: Timed not status
Description	This condition counts the attempts by users from the same device (the device from which this attempt is coming in) in the last few seconds whose authentication status is not the one given in the condition. If this count exceeds the count configured in the condition, then this condition evaluates to true.
Pre-Requisites	You should have this rule configured through a model.
Assumptions	
Available since version	10.1.4.5
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
status	We want to count the attempts with the status that is not equal to this status.	auth.status.enum (auth.status.enum.success is the default)	No
withinSeconds	This parameter defines the short period of time in which the number of login attempts into the system using that device are to be counted.	positive integer	No
attempts	Max number of attempts that we want to watch for. If the attempt count in Adaptive Risk Manager exceeds this number then condition will evaluate to true.	positive integer	No

Possible User Scenarios

This condition can be potentially used to determine if the device of the current activity is compromised. The possibility of fraud that can be detected here is someone (or a automated program) is using same device to make login attempts and they are either failing or passing based on what data the thieves have stolen. Or may be some program is trying to break the password for user in automated fashion. In these cases you would see repeated failed login attempt from same device in short amount of time.

A.1.1.9 DEVICE: Velocity from last login

Condition	DEVICE: Velocity from last login
Description	Condition evaluates if the users velocity in miles per hour is more than specified value. Location database is used to determine the location of the user for this login and previous login. Takes into account the current session also. Please note that the velocity calculation is highly dependent on accuracy of location data.
Pre-Requisites	You should have this rule configured through a model. Location database should be loaded to have correct behavior of this rule. You might also need tools (like browser header modifier plugin) to simulate the different IP for the incoming session.
Assumptions	Location database is loaded.
Available since version	10.1.4.5
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
milesPerHour	Positive number that indicates users speed in miles per hour. If condition determines that user has travelled faster than this value then condition will evaluate to true.	positive integer (default = 60)	No
sinceSeconds	This is a parameter that is a positive integer that specifies the time difference between this login and last login to calculate users velocity.	positive integer (default = 172800 which is 48 hours)	No

Possible User Scenarios

This condition can be used to determine users's location and risk it poses because of changes in user's login location from time to time.

One of the simplest scene is when user is traveling by ground transportation, you can configure this rule to be having typically having miles per hour as 60 and time to be in seconds (use default values).

Other case could be users traveling on air transport. Here you can use different values (say 500 miles an hour) to make sure that login locations and speed are reasonable behavior.

However we should be aware that the velocity calculation depend highly on location databases.

A.1.2 Auto-learning Conditions

A.1.2.1 ENTITY: Entity is member of pattern bucket for firsttime in certain time period

Condition	ENTITY: Entity is member of pattern bucket for firsttime in certain time period
Description	Condition to check if this Entity is member of pattern bucket for firsttime in certain time period. First time is kind of a relative function here. So if you want to really track first time, then in rule / model configuration user years as the time period type and use a long value like 5 years or so.

Condition	ENTITY: Entity is member of pattern bucket for firsttime in certain time period
Pre-Requisites	You should have entities and patterns defined before you try to add this to rule / model.
Assumptions	Auto Learning is enabled.
Available since version	10.1.4.5
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
Pattern Name for bucket firsttime	Name of the pattern for whose bucket firsttime is to be checked.		Cannot be null.
Is Condition true	Evaluate this condition to true if this parameter is true and firsttime bucket is true.		Cannot be null
Time period type for bucket membership	The time period Type (hours, days, months of years)	One of wotk.type.enum. That is (hour, day, month, year)	Cannot be null.
Time period for bucket membership	The time period over which the pattern membership is to be evaluated. This is just units of time	positive number. (Try to use sensible numbers depending on time period type). Use 0..24 for hours, use 1 through 12 for months, 1 through 31 for days, and 1 through 8 for years.	Cannot be null
Member type for pattern-bucket membership	The member Type (user, device, location, city, country)	It is one of the type of members applicable for that transaction. For authentication type it is one of user, device, IP, city, state, country.	Cannot be null.
First time Count	The count of occurrences against which to compare	If you are using this rule in Pre-Auth (or pre-transaction) scenario then use value of 0 here since auto learning takes place on trailing edge of authentication or transaction. For all other runtimes use value of 1 for this parameter. (1 is also a default value)	Cannot be null

Possible User Scenarios

Here are couple of examples of how to make use of this condition.

1] This condition can be potentially used in coming out with a first time rules. As an example define a user (city for each) pattern and attach this pattern to this condition based rule in a model. So when user comes in from a city first time, rule will be triggered.

2] This can be used for challenge users when they do something for first time in transactions also. For example user tried to do a bill transfer of 5000 dollars. This can be achieved using pattern that has user (transaction amount ranges 1..100, 1000...10000 etc.

A.1.2.2 ENTITY: Entity is member of pattern less than some percent times in given time period.

Condition	ENTITY: Entity is member of pattern less than some percent times in given time period.
Description	Condition to check if this Entity is member of pattern bucket for less than certain percent in certain time period.This condition checks the pattern membership percent against the pattern usage of same entity. Here we will be counting entity's membership count for percentage and not the number of entities that belong to that pattern.
Pre-Requisites	You should have entities and patterns defined before you try to add this to rule / model.
Assumptions	Auto Learning is enabled.
Available since version	10.1.4.5
RunTimes	All RunTimes

Parameters

Parameter	Description	Possible Values	Can be Null?
Pattern Name	Name of the pattern-bucket for whose percentage is to be checked.		Cannot be null
Is Condition true	Evaluate this condition to true if this parameter is true and the pattern percent is less than the given value		Cannot be null
Time period type for bucket membership	The time period Type (hours, days, months of years)	One of wotk.type.enum. That is (hour, day, month, year)	Cannot be null.
Time period for bucket membership	The time period over which the pattern membership is to be evaluated. This is just units of time	positive number. (Try to use sensible numbers depending on time period type). Use 0..24 for hours, use 1 through 12 for months, 1 through 31 for days, and 1 through 8 for years.	Cannot be null
Member type for pattern-bucket membership	The member Type (user, device, location, city, country)	It is one of the type of members applicable for that transaction. For authentication type it is one of user, device, IP, city, state, country.	Cannot be null.
patternHitPercent	The percentage to be compared.	Here again make sure you pass good values. Providing values in decimal points may not be a good idea. Since the percentage values may be Double type of values when calculated over a large number of login an pattern usage combination. So try to keep away from entering 10.45362. Rather go for 10.5 or I would suggest even just use 10 or 11 if you are not very picky about the exact number.	Cannot be null

Possible User Scenarios

This can be most effectively used in tracking user's own habits. Examples can be if user usually login from certain state and he started using other couple of states also. In that case he will be challenged on first few times he logs in from those states since his percentage for those state will be lower than say 10%. User (for each state) pattern can be used to achieve this.

A.1.2.3 ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture

Condition	ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture
Description	Condition to check if this Entity is member of pattern bucket some percent of time as compared to all other entities that have been member of this pattern. This condition takes into account all the other entities, so while making use of this condition, there will be obviously a bit of performance hit as compared to some simpler conditions.
Pre-Requisites	You should have entities and patterns defined before you try to add this to rule / model.
Assumptions	Auto Learning is enabled.
Available since version	10.1.4.5
RunTimes	All RunTimes

Parameters

Parameter	Description	Possible Values	Can be Null?
Pattern Name	Name of the pattern for whose bucket percentage is to be checked.		Cannot be null.
Is Condition true	Evaluate this condition to true if this parameter is true and percentage is less than the specified percentage.		Cannot be null
Time period type for bucket membership	The time period Type (hours, days, months of years)	One of wotk.type.enum. That is (hour, day, month, year)	Cannot be null.
Time period for bucket membership	The time period over which the pattern membership is to be evaluated. This is just units of time.	positive number. (Try to use sensible numbers depending on time period type). Use 0..24 for hours, use 1 through 12 for months, 1 through 31 for days, and 1 through 8 for years.	Cannot be null
Member type for pattern-bucket membership	The member Type (user, device, location, city, country)	It is one of the type of members applicable for that transaction. For authentication type it is one of user, device, IP, city, state, country.	Cannot be null.
percentHitCount	The percentage which we want to compare against.	Try to use a sensible number here. Use 10 or 11 in place of 10.7623591 as an example.	Cannot be null

Possible User Scenarios

This condition can be used to find out if users are doing something that is not in line with other using doing. For example user coming from a city that usually most users don't come in from.

Non popular states, cities, non-popular IPs etc. can be implemented using these condition.

A.1.2.4 ENTITY: Entity is member of pattern N times

Condition	ENTITY: Entity is member of pattern N times
Description	Condition to check if this Entity is member of pattern n number of times in last some time period.
Pre-Requisites	You should have entities and patterns defined before you try to add this to rule / model.
Assumptions	Auto Learning is enabled.
Available since version	10.1.4.5
RunTimes	All Runtimes, see the note for Pre-Auth though.

Parameters

Parameter	Description	Possible Values	Can be Null?
Pattern Name	Name of the pattern for whose bucket bucket membership is to be checked.		Cannot be null.
patternHitCountForUser	The hit count which will be compared against. If hit count for the pattern is more than this value then condition returns true.	For Pre-Auth execution set the count one less than what you want the rule to trigger on.	Cannot be null
Time period type for bucket membership	The time period Type (hours, days, months of years)	One of wotk.type.enum. That is (hour, day, month, year)	Cannot be null
Time period for bucket membership	The time period over which the pattern membership is to be evaluated. This is just units of time	positive number. (Try to use sensible numbers depending on time period type). Use 0..24 for hours, use 1 through 12 for months, 1 through 31 for days, and 1 through 8 for years.	Cannot be null
Member type for pattern-bucket membership	The member Type (user, device, location, city, country)	It is one of the type of members applicable for that transaction. For authentication type it is one of user, device, IP, city, state, country.	Cannot be null.
isMoreThan	Boolean value that is used to return true or false from condition. It works as below if (isMoreThan == true) and (hitCountMorethan returned true) then condition evaluates to true. ELSE if (isMoreThan == false) and (hitCountMorethan returned false) then condition evaluates to false. and condition evaluates to false in all other cases.		Cannot be null

Possible User Scenarios

This can be used to see if user performed a particular operation a few times, which was well defined. For example if user came in from a group of IP that are tagged as anonymizer. If user does it few times then model can be configured to take some action.

A.1.2.5 ENTITY Entity is member of bucket N times in a given time period

Condition	ENTITY: Entity is member of bucket N times in a given time period
Description	Condition to check if this Entity is a member of the bucket a number of times in a given time period. This condition can be used to check the current behavior against the pattern. Please note that this is a count-based condition. So, if you configure to trigger it, for example, for a count less than three, it will trigger on the first login that matches the fingerprint.
Pre-Requisites	Ensure that the following pre-requisites are met: ■ 10.1.4.5.2 or later must be installed. ■ Entities and patterns must be defined before adding this condition to rules/ models.
Assumptions	Auto-Learning is enabled.
Available since version	10.1.4.5.2
Runtimes	All runtimes see the note for pre-auth though.

Parameters

Parameter	Description	Possible Values	Can be Null?
Pattern Name	Name of the pattern for whose bucket membership is to be checked. In the rule / model UI select it from a drop down of active patterns that will be presented.		Cannot be null.
Time period for bucket membership	The time period over which the bucket membership is to be evaluated. This is in units of time.	Use 1 thru 23 for hours. 1 thru 30 for days. 1 thru 12 for months and 1 thru 8 for years. Server will use the use the max values if you enter values more than the above specified.	Cannot be null
Time period type for bucket membership	The time period Type (hours, days, months of years)	One of workflow.type.enum. That is (hour, day, month, year)	Cannot be null
Member type for pattern-bucket membership	The member Type (user, device, location [city, state, country], IP)	It is one of the type of members applicable for that transaction. For authentication type it is one of user, device, IP, city, state, country.	Cannot be null

Parameter	Description	Possible Values	Can be Null?
BucketHitCountForEntity	The hit count which will be compared against. Hit count for the bucket and the compare operator described below evaluate the outcome of the condition together.	For Pre-auth execution set the count one less than what you want the rule to trigger on.	Cannot be null
compareOperator	Comparison operator to be used for comparing the count in the system with bucketHitCountForEntity. For example if you passed compareoperator as "less_ than" and bucketHitCount as 3. Then if in the system the condition will evaluate to true as ling as hit count for that bucket is less than 3 for that authentication.	Possible values are picked up from enum bharosa.numeric.eval.operator.enum equal_to not_equal_to less_than less_than_or_equal_to more_than more_than_or_equal_to are the possible values.	Cannot be null.
successReturnValue	Value to return if the condition evaluates to true. If condition does not evaluate to true then opposite of the success value will be returned.	True / False.	Cannot be null
errorReturnValue	This is the value that will returned if the condition execution runs into issue. Some of the possible errors that it can run into is, pattern is not active, the parameters that were passed (configured) are incorrect or do not have the values in the expected range.	True / False.	Cannot be null.

Possible User Scenarios

This condition can be used to check if the user performed a particular operation a few times, which was well defined. For example if a user came in from a city for a few times, we can use this information to challenge the user for the first few times.

A.1.3 Location Conditions

A.1.3.1 LOCATION: ASN in group

Condition	LOCATION: ASN in group
Description	Check to see if the ASN for this IP location is in the group of ASNs that might be of interest. ASN is autonomous system number.
Pre-Requisites	There should a list of ASNs already defined. You should have this rule configured through a model.
Assumptions	

Condition	LOCATION: ASN in group
Available since version	
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
isInList	This is a boolean parameter that defines a default return value if the ASN is in the list.	[True] / False	Yes.
listId	This is a list id of the list of ASNs. The model -rule user interface will show you a menu of possible lists of ASNs to configure for this parameter. Please use group editor in Adaptive Risk Manager to edit the ASN list.		Yes

Possible User Scenarios

This condition can be potentially used to determine if the ASN of the current activity (IP) belongs to a particular list of ASNs. For example you might have certain ASNs those can be deemed as dangerous and you may want to block users coming in from there. Or you might not want users to do certain activity if they are coming in from an ASN that is from a particular country or region.

A.1.3.2 LOCATION: IP in Range group

Condition	LOCATION: IP in Range group
Description	Checks whether the IP of the current activity belongs to a list of IP-ranges specified.
Pre-Requisites	There should a group defined already which has IP-ranges as members. You should have this rule configured through a model.
Assumptions	
Available since version	10.1.4.5.1
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
isIPInRangeGroup	This is a boolean parameter that defines a default return value if the IP is really in range group.	[True] / False	Yes.
ipRangeListId	This is a list id of the list of IP-ranges. The model -rule GUI will show you a menu of possible lists of IP-ranges. Please use group editor in Adaptive Risk Manager to edit this group list.		Yes

Possible User Scenarios

This condition can be potentially used to determine if the IP of the current activity belongs to one of several ranges of IPs that may be of interest. For example you might

have ranges of IPs coming in from particular subnet and you might want to take some action if that is the case.

A.1.4 Transactions Conditions

Note: The filter operators "like" and "not like" work only on transaction data and entity data where the data type is string.

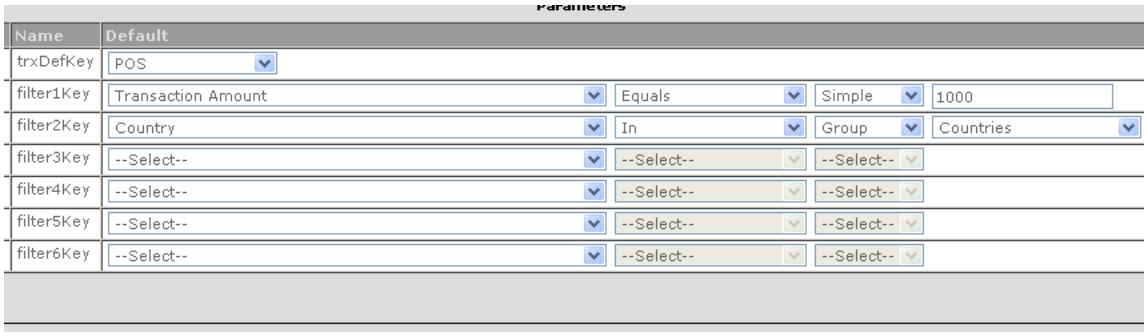
A.1.4.1 TRANSACTION: Check Current Transaction Using Filter Condition

Condition	TRANSACTION: Check Current Transaction Using Filter
Description	Check to see if the current transaction matches ALL the conditions specified. Up to 6 conditions can be specified.
Pre-Requisites	1. Transactions should be defined. 2. Transaction type of the current transaction should be the same as the transaction type specified in the rule condition
Assumptions	If there are multiple transactions in the current session, then this condition is applied on the last transaction
Available since version	10.1.4.5.1
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction type of the transaction to be counted. It represents the Transaction Definition fully qualified key. This is specified using the list box that has the list of transaction definitions		No
filter1Key filter2Key filter3Key filter4Key filter5Key filter6Key	These parameters specify the left hand side of the filter conditions. The left hand side represents the fully qualified key of the transaction field. This field could be an entity field or data field or transaction attribute or request attribute.		Yes

Parameter	Description	Possible Values	Can be Null?
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. The operator and the right hand side represent the fully qualified key of the filter condition. The right hand side is the value, which could be a simple value, the value of the current transaction, or a group. ■ Value: A simple value that is entered into a field ■ Current: A value from the current transaction. A value is selected from a list of values based on the current entities. ■ Group: Group is automatically selected if you chose the condition as IN or NOT IN. After Group is selected, you will have to select a type of group. Then, based on type, a list box appears with other values to select from, and so on.		Wherever the filterKey is specified, an appropriate condition has to be specified



Possible User Scenarios

This condition can be used whenever you want to trigger some rule based on checks on the current transaction.

For example, you have configured a transaction called purchase and you want to trigger a rule whenever the amount field of the purchase transaction is greater than 1000 and country is in the list of High Risk countries (that you have configured).

For achieving this, you need to use this rule with two filter conditions. One for checking if the amount field is greater than 1000 and the second filter condition for checking if the country of the current session is in the list of High Risk countries.

This condition can be used to specify up to six (6) filter conditions on the current transaction.

A.1.4.2 TRANSACTION: Check Transaction Count Using Filter Condition

Condition	TRANSACTION: Check Transaction Count Using Filter
Description	Check the transaction count with a specified value. You can specify the criteria for the transaction to be counted using the filter conditions (up to 6 conditions) and you can also specify the other parameters like the duration to be considered and the transaction status to consider etc.

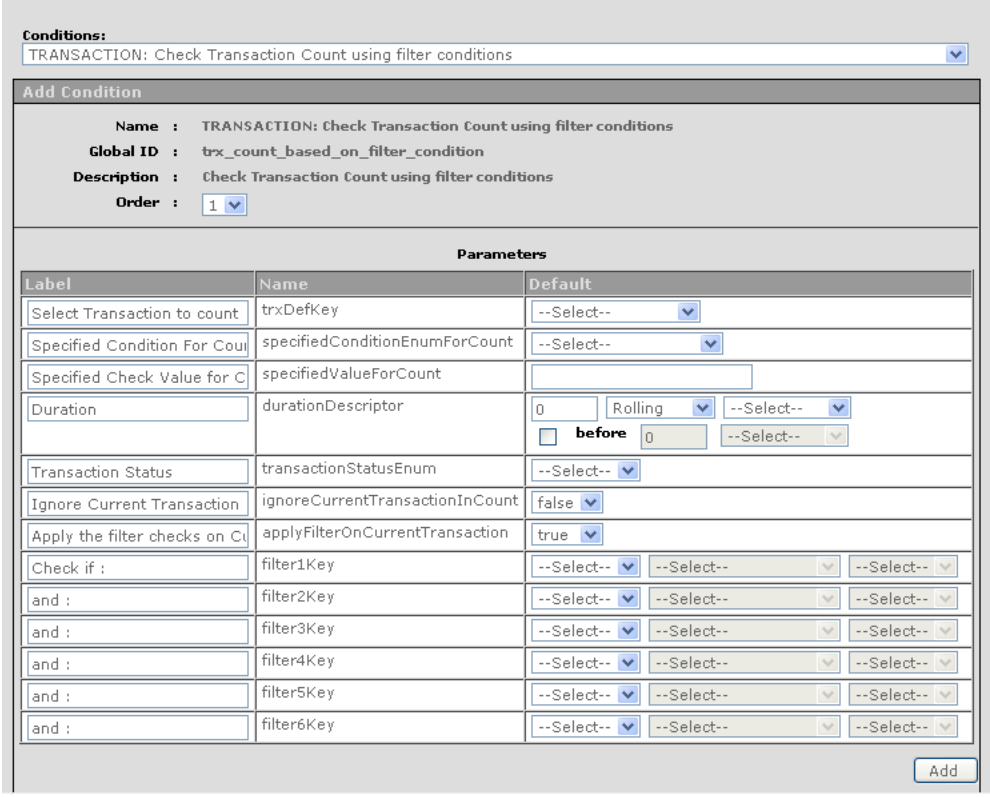
Condition	TRANSACTION: Check Transaction Count Using Filter
Pre-Requisites	■ Transactions should be defined. ■ Transaction type of the current transaction should be same as the transaction type specified in the rule condition
Assumptions	If there are multiple transactions in the current session, then this condition is applied on the last transaction
Available since version	10.1.4.5.1
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction type of the transaction to be counted. It represents the Transaction Definition fully qualified key. This is specified using the list box that has the list of transaction definitions		No
specifiedConditionEnumForCount	Operator to be applied for the count condition. Specify greater than, greater than or equals, less than, less than or equals		No
specifiedValueForCount	Transaction count numeric value to check		No

Parameter	Description	Possible Values	Can be Null?
durationDescriptor	Specify the duration during which the transactions have to be counted. The duration descriptor allows you to specify the duration. **Important:** By default, durationType is "rolling," meaning it takes the current time as the end point to count backwards to the start point. Whenever the duration is described as "last" x seconds/minutes/hours/days, the rolling type duration has to be used. So if you specify 1 day using "rolling" durationType, the "rolling" day starts 24 hours (exactly 1 day) from the current time. For example, if it is 11:33 am, and you specify 1 day, the "rolling" day will start from 11:33 am of the previous day and end at the current time today. There will be occasions where you want to have the duration window start at 0.00. For those occasions, you should use the durationType as "calendar". So if you specify 1 day using "calendar" as the durationType, the "calendar" day will start at 0.00 (12:00 am) of that day and end at the current time. Examples of "rolling" and "calendar": A "calendar" week starts from Sunday regardless of the current day, whereas the "rolling" week starts from 7 days from the current day. A "calendar" month starts from the 1st of the current month, whereas the "rolling" month starts from the same day of the previous month. A "calendar" year starts from January 1st of the current year, whereas the "rolling" year starts from the same day of the previous year. In both the "calendar" and "rolling," the end date/time is the current time. The durationType affects how the startTime of the duration is computed. The "Before" option is used when you want to skip over an interval of time before you begin counting backwards to the start point. For example, if you want to calculate 7 days worth of data, but you do not want the data from the last 7 days, you would specify the interval of time you want to skip. If today is February 6, and you want to look at data from January 17 to the 23rd, you would specify "Before" 15 days.		No

Parameter	Description	Possible Values	Can be Null?
transactionStatusEnum	Specify the transaction status that has to be considered for counting. Do not specify any status if you want to consider all transactions regardless of their status.		Yes
ignoreCurrentTransactionInCount	Specify if you want to ignore the current transaction (if any) in the count. If there are multiple transactions and if this is specified as true, only the last transaction is ignored.		Yes
applyFilterOnCurrentTransaction	Specify if you want to check the filter conditions on the current transaction before performing the count. If the filter conditions fail on the current transaction, then the rule condition is evaluated to false without performing the count.		
filter1Key filter2Key filter3Key filter4Key filter5Key filter6Key	These parameters specify the left hand side of the filter conditions. The left hand side represents the fully qualified key of the transaction field. This field could be an entity field or data field or transaction attribute or request attribute.		Yes
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. The operator and the right hand side represent the fully qualified key of the filter condition. The right hand side is the value, which could be a simple value, the value of the current transaction, or a group. ■ Value: A simple value that is entered into a field ■ Current: A value from the current transaction. A value is selected from a list of values based on the current entities. ■ Group: Group is automatically selected if you chose the condition as IN or NOT IN. After Group is selected, you will have to select a type of group. Then, based on type, a list box appears with other values to select from, and so on.		Wherever the filterKey is specified, appropriate condition has to be specified



Possible User Scenarios

This condition can be used whenever you want to trigger some rule based on transaction count condition.

For example, suppose you have configured a transaction called purchase and you want to challenge if a user is performing a lot of purchases (for example more than 2 per hour with amount > 1000 for each purchase) from a high risk country, you may want to use this condition.

For achieving this, you need to use this rule with the following:

1. Specify Count condition as 'Greater Than Equals'
2. Specify Count to check as '2'
3. Specify the duration with durationType as rolling and duration as 1 hour
4. Specify false for "Ignore Current Transaction in count?" since you want to consider current transaction in count
5. Specify true for "Apply FilterOnCurrentTransaction?" field
6. Two filter conditions.
   - One for checking if the amount field is greater than 1000
   - and the second filter condition for checking if the country of the current session is in the list of High Risk countries.

This condition can be used to specify up to six (6) filter conditions that are applied on transactions that are considered for counting

A.1.4.3 TRANSACTION: Check Transaction Aggregrate And Count Using Filter

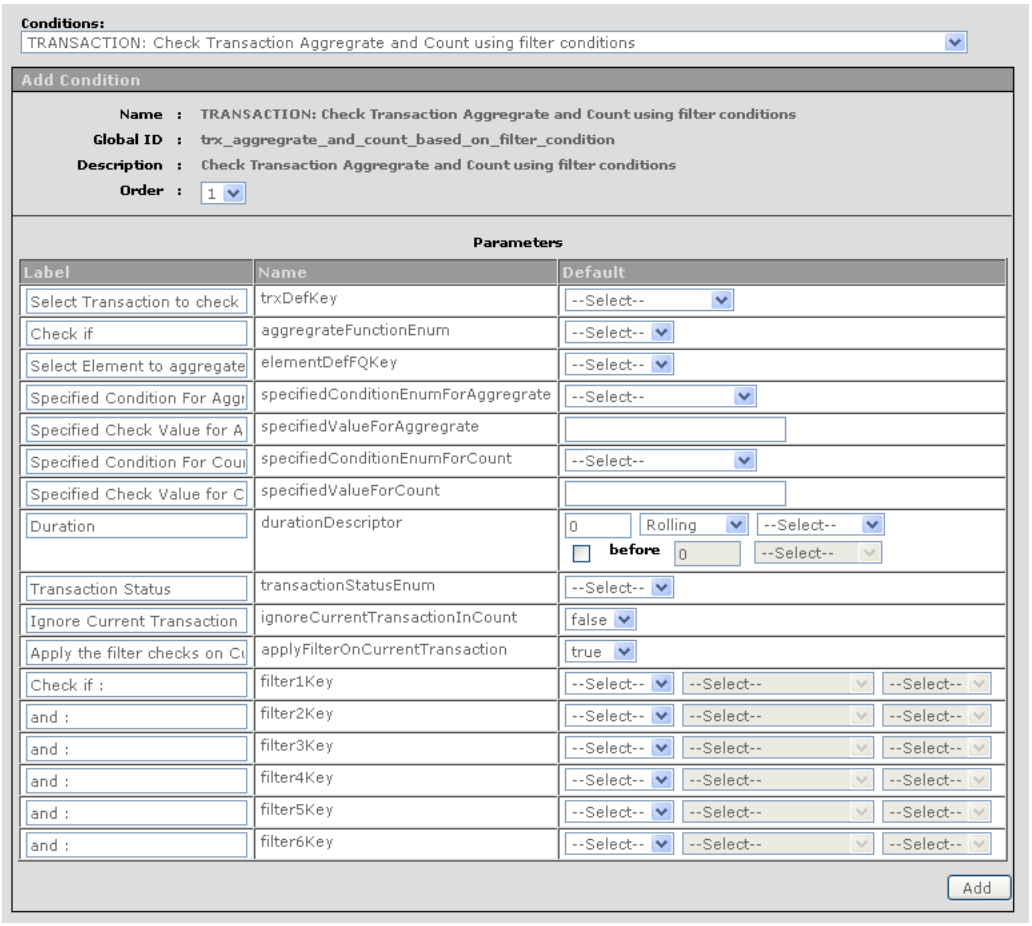
Condition	TRANSACTION: CheckTransactionAggregrateAndCountUsingFilter.xml
Description	Check the aggregrate of a numeric field and transaction count. You can specify the criteria for transaction to be counted using the filter conditions (up to 6 conditions) and you can also specify the other parameters like duration to be considered and the transaction status to consider etc.
Pre-Requisites	Transactions should be defined. Transaction type of the current transaction should be same as the transaction type specified in the rule condition
Assumptions	Aggregrate can be applied only on numeric fields. So the transaction definition should have at least one numeric field.
Available since version	10.1.4.5.1
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
aggregrateFunctionEnum	Aggregrate function to check. Available functions are sum, min, max, avg		
elementDefFQKey	Numeric element on which aggregrate check has to be performed. It represents fully qualified key of the numeric field. This is specified using list box that has list of all numeric data fields.		No
specifiedConditionEnumForAggregrate	Operator to be applied for the aggregrate condition. Specify greater than, greater than or equals, less than, less than or equals		No
specifiedValueForAggregrate	Aggregrate numeric value to check		No
specifiedConditionEnumForCount	Operator to be applied for the count condition. Specify greater than, greater than or equals, less than, less than or equals		Yes
specifiedValueForCount	Transaction count numeric value to check		Yes

Parameter	Description	Possible Values	Can be Null?
durationDescriptor	Specify the duration during which the transactions have to be counted. The duration descriptor allows you to specify the duration. **Important:** By default, durationType is "rolling," meaning it takes the current time as the end point to count backwards to the start point. Whenever the duration is described as "last" x seconds/minutes/hours/days, the rolling type duration has to be used. So if you specify 1 day using "rolling" durationType, the "rolling" day starts 24 hours (exactly 1 day) from the current time. For example, if it is 11:33 am, and you specify 1 day, the "rolling" day will start from 11:33 am of the previous day and end at the current time today. There will be occasions where you want to have the duration window start at 0.00. For those occasions, you should use the durationType as "calendar". So if you specify 1 day using "calendar" as the durationType, the "calendar" day will start at 0.00 (12:00 am) of that day and end at the current time. Examples of "rolling" and "calendar": A "calendar" week starts from Sunday regardless of the current day, whereas the "rolling" week starts from 7 days from the current day. A "calendar" month starts from the 1st of the current month, whereas the "rolling" month starts from the same day of the previous month. A "calendar" year starts from January 1st of the current year, whereas the "rolling" year starts from the same day of the previous year. In both the "calendar" and "rolling," the end date/time is the current time. The durationType affects how the startTime of the duration is computed. The "Before" option is used when you want to skip over an interval of time before you begin counting backwards to the start point. For example, if you want to calculate 7 days worth of data, but you do not want the data from the last 7 days, you would specify the interval of time you want to skip. If today is February 6, and you want to look at data from January 17 to the 23rd, you would specify "Before" 15 days.		No

Parameter	Description	Possible Values	Can be Null?
transactionStatusEnum	Specify the transaction status that has to be considered for counting. If you want to consider all transactions regardless of their status, do not specify any status		Yes
ignoreCurrentTransactionInCount	Specify if you want to ignore current transaction (if any) in the count. If there are multiple transactions and if this is specified as true, only the last transaction is ignored.		Yes
applyFilterOnCurrentTransaction	Specify if you want to check the filter conditions on the current transaction before performing the count. If the filter conditions fail on the current transaction then the rule condition is evaluated to false without performing the count.		
filter1Key filter2Key filter3Key	These parameters specify the left hand side of the filter conditions. The left hand side represents the fully qualified key of the transaction field.		
filter4Key filter5Key filter6Key	This field could be an entity field or data field or transaction attribute or request attribute.		
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. The operator and the right hand side represent the fully qualified key of the filter condition. The right hand side is the value, which could be a simple value, the value of the current transaction, or a group. ■ Value: A simple value that is entered into a field ■ Current: A value from the current transaction. A value is selected from a list of values based on the current entities. ■ Group: Group is automatically selected if you chose the condition as IN or NOT IN. After Group is selected, you will have to select a type of group. Then, based on type, a list box appears with other values to select from, and so on.		Wherever the filterKey is specified, appropriate condition has to be specified



Possible User Scenarios

This condition can be used whenever you want to trigger some rule based on aggregrate of a transaction numeric value and transaction count.

This is designed to reduce number of conditions since you can specify checks for both aggregrate and count in a single condition

For example, suppose you have configured a transaction called purchase and you want to challenge if a user is performing lot of purchases (for example, more than 2 per hour with average amount > 500) from a high-risk country.

For achieving this, you need to use this rule with the following:

1. Specify Aggregrate condition as 'Average'
2. Specify Aggregrate value to check as '500'
3. Specify Count condition as 'Greater Than Equals'
4. Specify Count to check as '2'
5. Specify the duration with durationType as rolling and duration as 1 hour
6. Specify false for "Ignore Current Transaction in count?" since you want to consider current transaction in count
7. Specify true for "Apply FilterOnCurrentTransaction?" field

8. One filter condition: for checking if the country of the current session is in the list of High Risk countries.

This condition can be used to specify up to six (6) filter conditions that are applied on transactions that are considered for counting

A.1.4.4 TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions

Condition	TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions
Condition	TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions
Description	Check to see if the count of a transaction entity or entity/data element with a given count where transactions matches ALL the conditions specified. Up to 6 conditions can be specified.
Pre-Requisites	Ensure that you are using 10.1.4.5.2 or later. Transactions should be defined; Transaction type of the current transaction should be same as the transaction type specified in the rule condition
Assumptions	
Available since version	10.1.4.5.2
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions		No
elementDefFQKey	Transaction Entity/Element that needs to be counted for checking		No
durationDescriptor	Duration Descriptor		No
forTheSameCurrentUserId	Boolean flag to indicate whether only transactions belonging to the current user to be counted or not		Yes
ignoreCurrentTransactionInCount	Flag to indicate if the current transaction has to be ignored in the count		
specifiedConditionEnumForCount	Condition for the count check. Select only valid operators that are relevant to numeric values		No
specifiedValueForCount	Count value to check. Specify only valid positive integers.		No
applyFilterOnCurrentTransaction	Flag to indicate if the filter conditions have to validated on current transaction before doing the count		No

Parameter	Description	Possible Values	Can be Null?
filter1Key filter2Key filter3Key	These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.		Yes
filter4Key filter5Key filter6Key	This field could be an entity field or data field or transaction attribute or request attribute. Note: There is a widget for this that renders list box with all the data fields.		
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition. Note: There is a widget for this that renders the list box of operators and a way to specify simple value or group name (in case of IN or NOT IN operator) or select another field in the transaction.		Wherever the filterKey is specified, appropriate condition has to be specified

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on the count of an entity or entity/data element of the transaction.

For example, you have configured a transaction called purchase and you want to trigger a rule if the same user is trying to use more than 5 different credit cards in the last 2 hours and the amount of purchase is more than $100.

To achieve this,

1. Select the "Credit Card" "Entity" name as the one to be counted, so that the rule counts the distinct number of credit cards used
2. Then select "For the same current user" flag as true.
3. Then select the duration as 2 Rolling hours and filter condition as "Amount" Greater Than 100.

There is provision to specify up to six (6) conditions for filtering the transactions that need to be considered for counting.

A.1.4.5 TRANSACTION: Check if consecutive Transactions in given duration satisfy the filter conditions

Condition	TRANSACTION: Check if consecutive Transactions in given duration satisfy the filter conditions
Description	Check if consecutive transactions in a given duration satisfy the specified filter conditions
Pre-Requisites	■ Transactions should be defined ■ Transaction type of the current transaction should be same as the transaction type specified in the rule condition ■ Ensure that you are using 10.1.4.5.2 or later.
Assumptions	

Condition	TRANSACTION: Check if consecutive Transactions in given duration satisfy the filter conditions
Available since version	10.1.4.5.2
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions		No
durationDescriptor	Duration Descriptor		No
transactionStatusGroupId	Group of Transaction Statuses that should be considered. If no group is specified then Transaction Status is ignored in the query.		Yes
ignoreCurrentTransactionInQuery	Flag to indicate if the current transaction has to be ignored		
forTheSameCurrentUserId	Flag to indicate if only transactions belonging to the current user to be counted. If this flag is false then transactions irrespective of users will be considered.		No
allowGapsForChecks	Flag to indicate if gaps are allowed while checking for conditions. If this value is TRUE then gaps would be allowed while checking for conditions.		No
noOfTransactionsToCheckFor1stCheck	Number of transactions that should satisfy the 1st check. Specify positive integers.		No
filter101Key	Filter Keys for 1st check.		Yes
filter102Key filter103Key filter104Key	These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.		
filter105Key filter106Key	This field could be an entity field or data field or transaction attribute or request attribute. Note: There is a widget for this that renders list box with all the data fields.		

Parameter	Description	Possible Values	Can be Null?
filter101Condition filter102Condition filter103Condition filter104Condition filter105Condition filter106Condition	Filter Conditions for 1st check. These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition. Note: There is a widget for this that renders the list box of operators and a way to specify simple value or group name (in case of IN or NOT IN operator) or select another field in the transaction.		Wherever the filterKey is specified, appropriate condition has to be specified
noOfTransactionsToCheckFor2ndCheck	Number of transactions that should satisfy the 2nd check. Specify positive integers.		No
filter201Key filter202Key filter203Key filter204Key filter205Key filter206Key	Filter Keys for 2nd check. These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field. This field could be an entity field or data field or transaction attribute or request attribute. Note: There is a widget for this that renders list box with all the data fields.		
filter201Condition filter202Condition filter203Condition filter204Condition filter205Condition filter206Condition	Filter Conditions for 2nd check. These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition. Note: There is a widget for this that renders the list box of operators and a way to specify simple value or group name (in case of IN or NOT IN operator) or select another field in the transaction.		Wherever the filterKey is specified, appropriate condition has to be specified

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on checks that are satisfied on consecutive transactions in a given duration.

For example, you have configured a transaction called purchase and you want to trigger a rule if the current/last transaction amount > $1000 and there were at least 3 transactions before that where the amount < $10.

So, rule is looking at the last 4 transactions and checking for a fraud pattern of small transactions first and then a big transaction.

Configure a rule with this rule condition and select the appropriate transaction type.

1. Select the number of transactions for 1st check as "1" and select the condition to check as "Amount" "Greater Than" 1000, since you want to check only one transaction for the big amount.

2. Select the number of transactions for 2nd check as "3" and select the condition to check as "Amount" "Less Than" 10, since you want to check 3 transactions for smaller amounts.
3. If you want to allow other transactions in between the checks for 1st check and 2nd check then select "Allow Gaps in Transactions during checks?" as TRUE otherwise select FALSE.

A.1.4.6 TRANSACTION: Compare Transaction Aggregrates (Sum/Avg/Min/Max) across two different durations

Condition	TRANSACTION: Compare Transaction Aggregrates (Sum/Avg/Min/Max) across two different durations
Description	Compare transactions aggregrates across two different durations
Pre-Requisites	▪ Transactions should be defined ▪ Transaction entity/data field that has to be aggregrated should be of type numeric ▪ Transaction type of the current transaction should be same as the transaction type specified in the rule condition ▪ Ensure that you are using 10.1.4.5.2 or later.
Assumptions	
Available since version	10.1.4.5.2
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions		No
aggregrateFunctionEnum	Aggregrate function that has to be used		No
elementDefFQKey	Transaction Entity/Data Element that needs to be aggregrated		No
durationDescriptorFor1stDuration	Select duration for the first aggregrate		No
durationDescriptorFor2ndDuration	Select duration for the second aggregrate		No
comparisonConditionEnum	Comparison condition		No
multiplierFor2ndDurationValue	Multiplier value for the second aggregrate. Only non-zero and null values will be considered		Yes
forTheSameCurrentUserId	Boolean flag to indicate whether only transactions belonging to the current user to be counted or not		Yes
ignoreCurrentTransactionInQuery	Flag to indicate if the current transaction has to be ignored		No

Parameter	Description	Possible Values	Can be Null?
specifiedConditionEnumForCount	Condition for the count check. Select only valid operators that are relevant to numeric values		No
specifiedValueForCount	Count value to check. Specify only valid positive integers.		No
applyFilterOnCurrentTransaction	Flag to indicate if the filter conditions have to validated on current transaction before doing the count		No
filter1Key filter2Key filter3Key	These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.		Yes
filter4Key filter5Key filter6Key	This field could be an entity field or data field or transaction attribute or request attribute. Note: There is a widget for this that renders list box with all the data fields.		
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition. Note: There is a widget for this that renders the list box of operators and a way to specify simple value or group name (in case of IN or NOT IN operator) or select another field in the transaction.		Wherever the filterKey is specified, appropriate condition has to be specified

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on the comparison of aggregrates of a transaction entity/data element across two different durations.

For example, you have configured a transaction called purchase and you want to trigger if sum of transaction amount for current day is 20% more than the sum of all transactions amount of previous day for that user.

To achieve this

1. Select the "Amount" as the element to be aggregrated and "Sum" as the aggregrate function.
2. Then select 1st duration as 1 calendar day and 2nd duration as 1 calendar day before 1 day.
3. Then select comparison condition as 'Greater than' and multiplier value as 1.2 (100%+20%).

A.1.4.7 TRANSACTION: Compare Transaction counts across two different durations

Condition	TRANSACTION: Compare Transaction counts across two different durations
Description	Compare transactions counts across two different durations
Pre-Requisites	▪ Transactions should be defined ▪ Transaction type of the current transaction should be same as the transaction type specified in the rule condition ▪ Ensure that you are using 10.1.4.5.2 or later.
Assumptions	
Available since version	10.1.4.5.2
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions		No
durationDescriptorFor1stDuration	Select duration for the first count		No
durationDescriptorFor2ndDuration	Select duration for the second count		No
comparisonConditionEnum	Comparison condition		No
multiplierFor2ndDurationValue	Multiplier value for the second aggregrate. Only non-zero and null values will be considered		Yes
forTheSameCurrentUserId	Boolean flag to indicate whether only transactions belonging to the current user to be counted or not		Yes
ignoreCurrentTransactionInCount	Flag to indicate if the current transaction has to be ignored		No
specifiedConditionEnumForCount	Condition for the count check. Select only valid operators that are relevant to numeric values		No
specifiedValueForCount	Count value to check. Specify only valid positive integers.		No
applyFilterOnCurrentTransaction	Flag to indicate if the filter conditions have to validated on current transaction before doing the count		No
filter1Key filter2Key filter3Key	These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.		Yes
filter4Key filter5Key filter6Key	This field could be an entity field or data field or transaction attribute or request attribute. Note: There is a widget for this that renders list box with all the data fields.		

Parameter	Description	Possible Values	Can be Null?
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition. Note: There is a widget for this that renders the list box of operators and a way to specify simple value or group name (in case of IN or NOT IN operator) or select another field in the transaction.		Wherever the filterKey is specified, appropriate condition has to be specified

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on the comparison of transaction counts across two different durations.

For example, you have configured a transaction called purchase and you want to trigger if the number of transactions for the current day is 20% more than the number of all transactions of the previous day for that user.

To achieve this,

1. Select 1st duration as 1 calendar day and 2nd duration as 1 calendar day before 1 day.
2. Then select the comparison condition as "Greater than" and multiplier value as 1.2 (100%+20%).

A.1.4.8 TRANSACTION: Compare Transaction Entity/Element counts across two different durations

Condition	TRANSACTION: Compare Transaction Entity/Element counts across two different durations
Description	Compare transaction entity/element counts across two different durations
Pre-Requisites	▪ Transactions should be defined ▪ Transaction type of the current transaction should be same as the transaction type specified in the rule condition ▪ Ensure that you are using 10.1.4.5.2 or later.
Assumptions	
Available since version	10.1.4.5.2
RunTimes	All Runtimes.

Parameters

Parameter	Description	Possible Values	Can be Null?
durationDescriptorFor1stDuration	Select duration for the first count		No
durationDescriptorFor2ndDuration	Select duration for the second count		No

Parameter	Description	Possible Values	Can be Null?
comparisonConditionEnum	Comparison condition		No
multiplierFor2ndDurationValue	Multiplier value for the second aggregrate. Only non-zero and null values will be considered		Yes
forTheSameCurrentUserId	Boolean flag to indicate whether only transactions belonging to the current user to be counted or not		Yes
ignoreCurrentTransactionInCount	Flag to indicate if the current transaction has to be ignored		No
specifiedConditionEnumForCount	Condition for the count check. Select only valid operators that are relevant to numeric values		No
specifiedValueForCount	Count value to check. Specify only valid positive integers.		No
applyFilterOnCurrentTransaction	Flag to indicate if the filter conditions have to validated on current transaction before doing the count		No
filter1Key filter2Key filter3Key	These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.		Yes
filter4Key filter5Key filter6Key	This field could be an entity field or data field or transaction attribute or request attribute. Note: There is a widget for this that renders list box with all the data fields.		
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition. Note: There is a widget for this that renders the list box of operators and a way to specify simple value or group name (in case of IN or NOT IN operator) or select another field in the transaction.		Wherever the filterKey is specified, appropriate condition has to be specified

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on the comparison of any transaction entity/element counts across two different durations.

For example, you have configured a transaction called purchase and you want to trigger if the number of distinct credit cards used in the current day is 20% more than the number of distinct credit cards used on the previous day for that user.

To achieve this,

1. Select "Credit card" as the element to be counted and select 1st duration as 1 calendar day and 2nd duration as 1 calendar day before 1 day.
2. Then select the comparison condition as "Greater than" and the multiplier value as 1.2 (100%+20%).

A.2 Mapping for configuring 10.1.4.3 rules using 10.1.4.5.2 rule conditions

Transaction Administration enables security policy administrators to more easily examine and evaluate transactional entities and define risk levels for transactions to proactively prevent fraud. The Transaction Administration feature was enhanced in 10.1.4.5. In 10.1.4.5.1 and 10.1.4.5.2, the transaction rule conditions were redesigned and simplified.

This section contains mapping information for users configuring their 10.1.4.3 rules using the 10.1.4.5.2 rule conditions.

A.2.1 DEVICE: Transaction Entity Count within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions

Mapping Notes:

1. In the rule condition select the required entity that needs to be counted and specify the count value that needs to be matched.
2. In the filter condition, select the "Device Id" as the left hand side, operator as 'Equals' and select the "Current" and "Device Id" from the right hand side drop down list.

A.2.2 LOCATION: Transaction Entity Count within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions

Mapping Notes:

1. In the rule condition select the required entity that needs to be counted and specify the count value that needs to be matched.
2. In the filter condition, select the "IP Address" as the left hand side, operator as 'Equals' and select the "Current" and "IP Address" from the right hand side drop down list.

A.2.3 USER: Transaction Status Count within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

1. Create a Transaction Status Group with required statuses
2. In the filter condition, select the "Transaction Status" as the left hand side, operator as 'IN' and select the appropriate Transaction Status Group.

A.2.4 USER: Transaction Total Amount within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

In the filter condition, select the amount field as the left hand side, operator as 'Greater Than' or other appropriate one and select the "Value" and enter the value to be matched.

A.2.5 USER: Transaction Data Count within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use the filter conditions and configure the conditions that should be satisfied for counting the transactions.

A.2.6 USER: Transaction amount more than specified on entity subtype between the time specified

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter conditions and configure the conditions involving time and entities.

Note: Time value should be specified in HH24:MI:SS format.

A.2.7 USER: Transaction Count within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

1. Select the duration using duration descriptor widget.
2. Use the filter conditions and configure the conditions that should be satisfied for counting the transactions.

A.2.8 USER: Transaction Entity Profile Data Count in Seconds

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions

Mapping Notes:

1. Select the entity to be counted and the specified comparison operator and specify count to be compared.

2. Select the duration using duration descriptor widget.
3. Use the filter conditions and configure the conditions that should be satisfied for counting the transaction entity.

A.2.9 USER: Transaction Profile Data Check Number Value

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition with the given transaction data element in the left hand side, appropriate operator and select "Value" from the drop down list and specify value to be compared with.

A.2.10 USER: Transaction Entity Id and Entity-Profile-Data in list

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition with the given entity and entity data element in the left hand side, "IN" operator and select "Group" from the drop down list and select appropriate Group.

A.2.11 USER: Transaction Entity Count and Total Amount within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Aggregrate and Count using filter conditions

Mapping Notes:

1. Specify the element to compare the aggregrate and specify the aggregrate value to be compared, also specify the count to be compared with.
2. Use filter conditions to narrow the transactions to be considered for computing the count and aggregrate.

A.2.12 USER: Transaction Profile Data check

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter conditions to configure the checks

A.2.13 USER: Check Transaction Data Count within duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions

Mapping Notes:

1. Select the entity/data element to be counted and the specified comparison operator and specify count to be compared.
2. Select the duration using duration descriptor widget.
3. Use the filter conditions and configure the conditions that should be satisfied for counting the transaction entity/data element.

A.2.14 USER: Transaction Profile Data Compare Values

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition and select the element to compare with on the left hand side and appropriate operator and the select element to be compared with on the right hand side.

A.2.15 USER: Transaction Data Count within specified duration with same data

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

1. Select the duration using duration descriptor widget.
2. Use the filter conditions and configure the condition with the elements to compare on the left hand side, operator as "Equals" and select "Current" and the element to be compared with.

A.2.16 USER: Transaction Entity Count and Total Amount within specified duration with specific profile data

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Aggregrate and Count using filter conditions

Mapping Notes:

1. Specify the element to compare the aggregrate and specify the aggregrate value to be compared, also specify the count to be compared with.
2. Select the duration using duration descriptor widget.
3. Use filter conditions and select the element to be matched on the left hand side, select operator and then select "Current" and the relevant element from current transaction data to be compared with.

A.2.17 USER: Transaction Entity and Entity-Profile-Data in lists

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition with operator IN to check for value in Groups/Lists.

A.2.18 USER: Transaction Entity Profile Different Data Count in Seconds

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions

Mapping Notes:

1. Select the entity/data element to be counted and the specified comparison operator and specify count to be compared.
2. Select the duration using duration descriptor widget.
3. Use the filter conditions and configure the conditions that should be satisfied for counting the transaction entity/data element.

A.2.19 USER: Transaction Entity Type Count within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions

Mapping Notes:

1. Select the entity to be counted and the specified comparison operator and specify count to be compared.
2. Select the duration using duration descriptor widget.
3. Use the filter conditions and configure the conditions that should be satisfied for counting the transaction entity

A.2.20 USER: Transaction Status Count within specified duration in sequence

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check if consecutive Transactions in given duration satisfy the filter conditions

Mapping Notes:

Transactions will be fetched and sorted in descending order of create time of transactions.

1. If "Ignore current Transaction in query" parameter is false then current transaction will be the first in the list of transactions.
2. Select the duration using duration descriptor widget.
3. Enter the number of transactions that should satisfy the first check and then use the 1st check filter conditions to specify the checks.
4. Enter the number of transactions that should satisfy the second check and then use the 2nd check filter conditions to specify the checks.
5. If gaps should be allowed before the 1st check or between 1st check and 2nd check then select the "Allow Gaps in Check?" parameter as TRUE.

A.2.21 USER: Transaction Profile Data In List

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition with operator IN to check for value in Groups/Lists.

A.2.22 USER: Transaction Entity Count Comparison within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Compare Transaction Entity or Element Counts across two different durations

Mapping Notes:

1. Select the entity/data element to be counted
2. Select the durations for 1st set and 2nd set of transactions using duration descriptor widgets
3. Specify the comparison condition and multiplier for the count value of 2nd set of transactions

A.2.23 USER: Transaction Count on an entity series within specified duration

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check if consecutive Transactions in given duration satisfy the filter conditions

Mapping Notes:

1. Select the duration using duration descriptor
2. Select the number of transactions to pass for the 1st check
3. Specify the 1st check that has to be passed using the filter conditions
4. If there is one more check, then specify the number of transactions for the 2nd check and use the filter conditions to specify that check

A.2.24 USER: All Transaction Data Match Count Sum Of Amount And Time

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Aggregrate and Count using filter conditions

Mapping Notes:

1. Specify the element to compare the aggregrate and specify the aggregrate value to be compared, also specify the count to be compared with.
2. Select the duration using duration descriptor widget.
3. Use filter conditions and select the element to be matched on the left hand side, select operator and then select "Current" and the relevant element from current transaction data to be compared with.

A.2.25 USER: All Transaction Entry Data Match Count Sum Of Amount And Time

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Aggregate and Count using filter conditions

Mapping Notes:

1. Specify the element to compare the aggregate and specify the aggregate value to be compared, also specify the count to be compared with.
2. Select the duration using duration descriptor widget.
3. Use filter conditions and select the element to be matched on the left hand side, select operator and then select "Current" and the relevant element from current transaction data to be compared with.

A.2.26 USER: All Transaction Entry Data Match Count Sum Of Amount And Time

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Aggregate and Count using filter conditions

Mapping Notes:

1. Specify the element to compare the aggregate and specify the aggregate value to be compared, also specify the count to be compared with.
2. Select the duration using duration descriptor widget.
3. Use filter conditions and select the element to be matched on the left hand side, select operator and then select "Current" and the relevant element from current transaction data to be compared with.

A.2.27 USER: Transaction Data Match And Amount Exceeds

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition and select the element to compare with on the left hand side and appropriate operator and the select element to be compared with on the right hand side.

A.2.28 USER: Transaction Data Match And Amount Exceeds 2

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition and select the element to compare with on the left hand side and appropriate operator and the select element to be compared with on the right hand side.

A.2.29 USER: Transaction Entity Profile Data older than specified time

Equivalent 10.1.4.5.2 Rule Condition:

Not directly available

Mapping Notes:

It is advised to use combination of "TRANSACTION: Check Current Transaction using the filter conditions" and "Session: Check param value" to achieve this.

A.2.30 USER: Transaction Entity Profile Specified Data And Amount

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition and select the element to compare with on the left hand side and appropriate operator and the select element to be compared with on the right hand side.

A.2.31 Session: Transaction type in time and value more than

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

1. Select count to check as "1" and count compare condition as "Greater Than Equals".
2. Select the duration using duration descriptor widget.
3. Use the filter conditions and configure the condition with the elements to compare on the left hand side, operator as "Greater Than" and select "Value" and specify the numeric value in text field.

A.3 Mapping for configuring 10.1.4.5 rules using 10.1.4.5.2 rule conditions

Transaction Administration enables security policy administrators to more easily examine and evaluate transactional entities and define risk levels for transactions to proactively prevent fraud. The Transaction Administration feature was enhanced in 10.1.4.5. In 10.1.4.5.1 and 10.1.4.5.2, the transaction rule conditions were redesigned and simplified.

This mapping section contains mapping information for users configuring their 10.1.4.5 rules using the 10.1.4.5.2 rule conditions.

A.3.1 TRANSACTION: Check Transaction Count for Current Entity

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

In the filter condition, select the required entity that needs to be matched as the left hand side, operator as 'Equals' and select the "Current" and the required Entity to match with from the right hand side drop down list.

A.3.2 TRANSACTION: Is the entity date element between specified dates

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the two filter conditions with the given entity date element in the left hand side and use "greater than equals" with the first date and "less than equals" with the second date.

Date values should be in the format in "mm/dd/yyyy HH24:MI:SS"

A.3.3 TRANSACTION: Is the entity element in specified duration

Not available yet

A.3.4 TRANSACTION: Is the given entity element is in the given list

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition with the given entity element in the left hand side, operator as IN and the required group/list on the right hand side.

A.3.5 TRANSACTION: Is the entity numeric element is in the given numeric range

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use two filter conditions with the given entity element in the left hand side and use "greater than equals" with the first value and "less than equals" with the second value.

A.3.6 TRANSACTION: Is the given transaction data element is in the given list

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the filter condition with the given transaction data element in the left hand side, operator as IN and the required group/list on the right hand side.

A.3.7 TRANSACTION: Is the transaction date element between specified dates

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use the two filter conditions with the given transaction date element in the left hand side and use "greater than equals" with the first date and "less than equals" with the second date.

Date values should be in the format in "mm/dd/yyyy HH24:MI:SS"

A.3.8 TRANSACTION: Is the transaction date element in specified duration

Not available yet

A.3.9 TRANSACTION: Is the transaction numeric data in the given numeric range

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Current Transaction using the filter conditions

Mapping Notes:

Use two filter conditions with the given transaction numeric element in the left hand side and use "greater than equals" with the first value and "less than equals" with the second value.

A.3.10 TRANSACTION: Check Transaction Count with specified count based on All of Current Entity Data Match

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the given entity on the left hand side and use "equals" operator and select "Current" and then the required entity that needs to be matched.

A.3.11 TRANSACTION: Check Transaction Count based on Current Entity Element Match with the specified count

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the given entity element on the left hand side and use "equals" operator and select "Current" and then the required entity element that needs to be matched.

A.3.12 TRANSACTION: Check Transaction Count with Specified Count based on Current Transaction Data Element Match

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the given transaction data element on the left hand side and use "equals" operator and select "Current" and then the required transaction data element that needs to be matched.

A.3.13 TRANSACTION: Check Transaction Count with Specified Count based on All of Current Transaction Data Match

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use as many filter conditions as the number of transaction data elements and in each filter condition, select the transaction data element on the left hand side and use "equals" operator and select "Current" and then the required transaction data element that needs to be matched.

A.3.14 TRANSACTION: Check Transaction Count based on Entity Element Match In List values with the specified count

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the given entity data element on the left hand side and use "IN" operator and select the required Group/List.

A.3.15 TRANSACTION: Check Transaction Count based on Entity Element Match with the specified count

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the given entity element on the left hand side and use appropriate operator and select "Value" and then enter the value to be matched.

A.3.16 TRANSACTION: Check Transaction Count with Specified Count based on Transaction Data Element Match In List values

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the given transaction data element on the left hand side and use "IN" operator and select the required Group/List.

A.3.17 TRANSACTION: Check Transaction Count with Specified Count based on Transaction Data Element Match

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the given transaction data element on the left hand side and use appropriate operator and select "Value" and then enter the value to be matched.

A.3.18 TRANSACTION: Check Transaction Count From Current Transactions' IPAddress with Specified Count

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the "IP Address" on the left hand side and use "equals" operator and select "Current" and "IP Address" from the drop down list.

A.3.19 TRANSACTION: Check Transaction Count From IPAddress with Specified Count

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Use one filter condition with the "IP Address" on the left hand side and use "equals" operator and select "Value" and enter the required "IP Address" to be matched in the text field.

A.3.20 TRANSACTION: Check Transaction Count with the specified count value

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Count using filter conditions

Mapping Notes:

Configure filter conditions if required.

A.3.21 TRANSACTION: Check Transaction Data Numeric Element Aggregrate with the Specified Value

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Aggregrate and Count using filter conditions

Mapping Notes:

Configure rule condition by selecting the required Transaction Data Element as the field to aggregrate. Leave the count value to be matched as NULL.

A.3.22 TRANSACTION: Check Transaction Entity Numeric Element Aggregrate with the specified value

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Transaction Aggregrate and Count using filter conditions

Mapping Notes:

Configure rule condition by selecting the required Transaction Entity Element as the field to aggregrate. Leave the count value to be matched as NULL.

A.3.23 TRANSACTION: Check Unique Transaction Entity Count with the specified count

Equivalent 10.1.4.5.2 Rule Condition:

TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions

Mapping Notes:

Configure rule condition by selecting the required Entity to be counted and specify the count value to be matched along with appropriate comparison operator.

If required use filter conditions to narrow down the transactions that need to be included for counting the entity.

B

Oracle Adaptive Access Manager Reports

This appendix lists the 52 Oracle Adaptive Access Manager BI Publisher reports along with their descriptions.

Case Reports

These reports provide data based on the case information.

- **CaseActivity**: lists the count of agent and CSR cases based on the case status for the specified date range.
- **Cases**: lists all cases based on case status and the date range specified.

Common Reports

These reports provide data based on device location or login information.

- **DeviceLocations**: lists the locations for a specific device.
- **RecentLogins**: lists all logins in the specified time range.

Devices Reports

These reports provide data based on the device information.

- **DeviceIdScoring**: displays device ID scoring summary for the designated date range.
- **DevicesByUser**: lists all devices for a given User.
- **FrequentLogins**: lists all devices with multiple logins in the specified time range.
- **InvalidUsers**: lists all devices with login attempts from invalid users occurring during the designated date range.
- **MultipleFailures**: lists all devices with multiple login failures in the specified time range.
- **MultipleSuccessfulLogins**: lists all devices with multiple successful logins.
- **MultipleUsers**: lists all devices that have multiple users.
- **NewDevices**: lists all new device IDs created in the specified time range.

KBA Reports

These reports provide data based on the KBA information.

- **ChallengeStatistics**: lists challenge response statistics.

  For example,

  Users with Failure counter > 0 - failures more than none (have at least failed once)

Users with multiple failures - failures more than one (have failed multiple times)

- **QuestionStatistics**: lists challenge question statistics.
- **Registration**: lists question registration statistics.

Location Reports

These reports provide data based on the location information.

- **CountryAggregates**: displays country aggregate summary for the designated date range.
- **FrequentLogins**: lists all locations with multiple logins in the specified time range.
- **InvalidUsers**: lists all the locations with login attempts from invalid users occurring during the designated date range.
- **MultipleLoginFailures**: lists all locations with multiple login failures in the specified time range.
- **MultipleLoginSuccess**: lists all locations with multiple successful logins.
- **MultipleUsers**: lists all locations that have multiple users.
- **RoutingAggregates**: displays routing aggregate summary for the designated date range.
- **StateAggregates**: displays state aggregate summary for the designated date range.
- **UserLocations**: lists all locations a user has attempted logins from.

Patterns Reports

These reports provide data based on the pattern information.

- **BucketsByPatternAndMember**: lists all buckets based on pattern and member type for the time range specified.
- **MemberEntitiesByPattern**: lists all metadata for the member entity based on the pattern selected.
- **MembersByPattern**: lists all members based on the pattern selected.
- **PatternsByMember**: lists all patterns available based on the Member Type.
- **PatternsByMemberEntities**: lists all patterns that have the specific metadata as its member entity.

Performance Reports

These reports provide data based on the performance information.

- **BlockedLoginsPerMinute**: lists the counts of blocked logins every five minutes in the last one hour time frame.
- **BlockedTransactionsPerMinute**: lists the counts of blocked transactions every five minutes in the last one hour time frame.
- **CommonAPIPerformance**: displays the Average Processing time and counts for Common API calls for the designated date range.
- **KBAChallengesPerMinute**: displays the KBA Challenge Results and the number of challenges for the designated date range.
- **LoginHighAlertsPerMinute**: displays the Logins with High Alerts and their counts for the designated date range.

- **RulesAPIPerformance**: displays the Average Processing time and counts for Rule API calls for the designated date range.
- **RulesPerformance**: displays the Average Processing time, runtime, and counts for the rules in the designated date range.
- **TrackerAPIPerformance**: displays the Average Processing time and counts for Tracker API calls for the designated date range.
- **TransactionsHighAlertPerMinute**: displays the Transactions with High Alerts and their counts for the designated date range.
- **TransactionsPerMinute**: displays the total number of Transactions every five minutes in the last one hour time frame.

Security Reports

These reports provide data based on the security information.

- **Alerts**: lists all alerts generated during the designated date range.
- **AlertsBreakdown**: displays alert breakdown summary for the designated date range.
- **PostAuthScoring**: displays post-auth scoring summary for the designated date range.
- **PreAuthScoring**: displays pre-authorization scoring summary for the designated date range.
- **RulesBreakdown**: displays rules breakdown summary for the designated date range.
- **ScoringCombinations**: displays score combination summary for the designated date range.

Summary Reports

These reports provide summaries for date ranges.

- **AveragesSummary**: displays average summary for the designated date range.
- **LoginSummary**: displays login aggregate summary for the designated date range.

Users Reports

These reports provide data based on the user information.

- **FirstLogin**: lists the first login attempt occurring during the designated date range for all users.
- **FrequentLogins**: lists all users with multiple logins in the specified time range.
- **InvalidLogins**: lists all login attempts from invalid users occurring during the designated date range.
- **MultipleDevices**: lists all users that use multiple devices.
- **MultipleFailures**: lists all users with multiple failures in the specified time range.

C

Universal Installation Option Actions

This appendix lists the Universal Installation Option actions.

Action	Description
Allow	Allow user to access the system.
Block	Does not allow user to access the system.
ChallengeHTML	Challenge user using HTML page instead of authentipad.
RegisterUserHTML	Register user using HTML page instead of authentipad.
RegisterUserOptionalHTML	Optional registration using HTML page instead of authentipad.
RegisterQuestionsHTML	Register questions using HTML page instead of authentipad.
ChallengeQuestionPad	Challenge user using QuestionPad.
ChallengeQuestionPadGeneric	Challenge user using QuestionPad that contains no personalization (image/phrase).
RegisterUserQuestionPad	Register user using QuestionPad.
RegisterUserOptionalQuestionPad	Optional registration using QuestionPad.
RegisterQuestionsQuestionPad	Register questions using QuestionPad.
RegisterQuestionsQuestionPadGeneric	Register questions using QuestionPad that contains no personalization (image/phrase).
ChallengeTextPad	Challenge user using TextPad.
RegisterUserTextPad	Register user using TextPad.
RegisterUserOptionalTextPad	Optional registration using TextPad.
RegisterQuestionsTextPad	Register questions using TextPad.
PasswordTextPad	Prompt user for password using TextPad.
PasswordTextPadGeneric	Prompt user for password using TextPad that contains no personalization (image/phrase).
PasswordTextPadFirstTime	Prompt user for password using TextPad for the first time.
PasswordTextPadGenericFirstTime	Prompt user for password using TextPad for the first time that contains no personalization (image/phrase).
ChallengePinPad	Challenge user using PinPad.
RegisterUserPinPad	Register user using PinPad.
RegisterUserOptionalPinPad	Optional registration using PinPad.
RegisterQuestionsPinPad	Register questions using PinPad.

Action	Description
PasswordPinPad	Prompt user for password using PinPad.
PasswordPinPadGeneric	Prompt user for password using PinPad that contains no personalization (image/phrase).
PasswordPinPadFirstTime	Prompt user for password using PinPad for the first time.
PasswordPinPadGenericFirstTime	Prompt user for password using PinPad for the first time that contains no personalization (image/phrase).
ChallengeKeypadFull	Challenge user using KeyPad.
RegisterUserKeyPadFull	Register user using KeyPad.
RegisterUserOptionalKeyPadFull	Optional registration using KeyPad.
RegisterQuestionsKeyPadFull	Register questions using KeyPad.
PasswordKeypadFull	Prompt user for password using KeyPad.
PasswordKeypadFullGeneric	Prompt user for password using KeyPad that contains no personalization (image/phrase).
PasswordKeypadFullFirstTime	Prompt user for password using KeyPad for the first time.
PasswordKeypadFullGenericFirstTime	Prompt user for password using KeyPad for the first time that contains no personalization (image/phrase).
ChallengeKeypadAlpha	Challenge user with Alphanumeric Keypad (numbers and letters only, no special characters)
RegisterUserKeyPadAlpha	Register user with Alphanumeric Keypad (numbers and letters only, no special characters)
RegisterUserOptionalKeyPadAlpha	Optional registration with Alphanumeric Keypad (numbers and letters only, no special characters)
RegisterQuestionsKeyPadAlpha	Register questions with Alphanumeric Keypad (numbers and letters only, no special characters)
PasswordKeypadAlpha	Prompt user for password with Alphanumeric Keypad (numbers and letters only, no special characters)
PasswordKeypadAlphaGeneric	Prompt user for password with Alphanumeric Keypad (numbers and letters only, no special characters) that contains no personalization (image / phrase)
PasswordKeypadAlphaFirstTime	Prompt user for password with Alphanumeric Keypad (numbers and letters only, no special characters) for the first time
PasswordKeypadAlphaGenericFirstTime	Prompt user for password with Alphanumeric Keypad (numbers and letters only, no special characters) for the first time with no personalization (image / phrase)
PasswordHTML	Prompt user for password using HTML page instead of an authentipad.
RegisterImageTextPad	Allow user to select image using TextPad.
RegisterImagePinPad	Allow user to select image using PinPad.
RegisterImageKeyPadFull	Allow user to select image using KeyPad.
RegisterImageKeyPadAlpha	Allow user to select image using Alphanumeric Keypad keyset (numbers and letters only)
RegisterImageQuestionPad	Allow user to select image using QuestionPad.
RegisterUserOptional	This is used in native integrations using "Sample" not in Universal Installation Option Deployments. In these environments, a separate runtime is run to determine the device to display; it is not embedded in the pre-auth rules return.

Action	Description
RegisterUser	This is used in native integrations using "Sample" not in Universal Installation Option Deployments. In these environments a separate runtime is run to determine the device to display; it is not embedded in the pre-auth rules return.

D

Account Statuses

The account statuses come from common_enum.properties and they are configurable.

vcrypt.user.account.status.enum.pending_activation.name=Pending Activation

The user started registration, but has not completed it. He has entered his username and password and his information has been stored in the database, but he will not be activated until he has completed registration. The user is available in the system, but he is not yet active and cannot perform any operations.

vcrypt.user.account.status.enum.active.name=Active

The user is active and available in the system. He has completed registration and can perform all operations.

vcrypt.user.account.status.enum.disabled.name=Disabled

The user is available in the system, but not active. He maybe disabled because of fraud or other reasons and cannot perform any operations.

vcrypt.user.account.status.enum.deleted.name=Deleted

The user is not available in the system.

vcrypt.user.account.status.enum.invalid.name=Invalid

The username is not valid.

E

Authentication Statuses

The authentication statuses come from bharosa_app.properties and they are configurable.

auth.status.enum.success.name=Success

The user is successfully authenticated.

auth.status.enum.invalid_user.name=Invalid user

The username was invalid and not available in the system.

auth.status.enum.wrong_password.name=Wrong password

The user entered the wrong password. The username was entered correctly, but the password was incorrect.

auth.status.enum.wrong_pin.name=Wrong pin

If user has pin as password and it was entered incorrectly.

auth.status.enum.session_expired.name=Session expired

The user logged in to the application then left it inactive for a length of time. When the user tries to use the application again, a message appears telling him the session has expired. The user will have to log in again.

auth.status.enum.session_reused.name=Session reused

When the session had expired and the user logged in successfully, the status changes from session expired to session reused.

auth.status.enum.user_disabled.name=User disabled

The user was available in the system, but had been disabled in the system for a variety of reasons. The username is valid, but he has been disabled.

auth.status.enum.pending_activation.name=Pending activation

The user has not completed the registration yet.

auth.status.enum.wrong_answer.name=Wrong Answer

The user entered the wrong answer to a challenge question.

auth.status.enum.db_error.name=Database Error

When user was performing a database operation, he encountered an error.

auth.status.enum.system_error.name=System Error

When user was using the application, he encountered an error.

auth.status.enum.block.name=Blocked

If a user is "Blocked," it is because a Model has found certain conditions to be "true" and is set up to respond to these conditions with a "Block Action." If those conditions change, the user may no longer be "Blocked." The "Blocked" status is not necessarily permanent and therefore may or may not require an administrator action to resolve. For example, if the user was blocked because he was logging in from a blocked country, but he is no longer in that country, he may no longer be "Blocked."

auth.status.enum.challenge_block.name=Locked

"Locked" is the status that Oracle Adaptive Access Manager sets if the user fails a question challenge. The "Locked" status is only used if the One-Time-Password (OTP) facility is in use. OTP sends a one-time password to the user via e-mail or SMS text message. If the user exceeds the number of retries when attempting to put in his OTP code, then his account becomes "Locked." After that, a Customer Service Representative must reset the status to "Unlocked" before the account can be used to enter the system.

auth.status.enum.pending.name=Pending

The user has logged into the application, completed registration, but the he did not go through the entire flow.

Glossary

Access Authentication

In the context of an HTTP transaction, the basic access authentication is a method designed to allow a web browser, or other client program, to provide credentials—in the form of a user name and password—when making a request.

Action

An event activated when a rule is triggered. For example: block access, challenge question, ask for PIN, and so on.

Agent Cases

Agent Cases are used specifically by fraud investigators and investigation managers for analyzing data and finding relationships between sessions and cases. When an investigator links sessions and cases, Oracle Adaptive Access Manager can search the data for suspicious activity.

Alert

A message generated when a rule is triggered. For example: login attempt from a new country for this user.

Application ID

The primary ID for the user. For example, a user can be part of "bharosauiogrp" and "testgrp," but his Application Id or primary ID will be "bharosauiogrp." Application ID is similar to a userid group.

Attribute

Adaptive Risk Manager will collect data on the attributes to be used in the pattern membership.

For example, if you pick "user" as the member type and the attributes: IP (NNN.N.N.N), City (Redwood City) and Is Registered (False); Adaptive Risk Manager will record when users match all of these attributes. This profiling can then be used to evaluate risk for the "user."

Authentication

The process of verifying a person's, device's, application's identity. Authentication deals with the question "Who is trying to access my services?"

Authorization

Authorization regards the question "Who can access what resources offered by which components?"

Auto-learning

Auto learning is a feature that analyzes the behavior of user data coming into the system and profiles (creates digest) of the user's data. This data is then stored in a historical data table and used for calculating the risk based on rules. The best advantage of Auto-learning is that the system learns the changes in user's behavior and slowly adapts to it when calculating risk.

Blocked

If a user is "Blocked," it is because a Model has found certain conditions to be "true" and is set up to respond to these conditions with a "Block Action." If those conditions change, the user may no longer be "Blocked." The "Blocked" status is not necessarily permanent and therefore may or may not require an administrator action to resolve. For example, if the user was blocked because he was logging in from a blocked country, but he is no longer in that country, he may no longer be "Blocked."

Bots

Software applications that run automated or orchestrated tasks on compromised PCs over the internet. An organization of bots is known as a bot net or zombie network.

Buckets

Buckets are groupings of behaviors.

Auto-learning patterns are used to dynamically create and populate profiling buckets to track behavior and transactions.

Buckets help in creating the statistics for the entities based on their memberships to various patterns and hour/day/month/year time samples.

Case Created

The date and time the case was created.

Case Description

The details for the case. A description is required for cases.

Case Number

A unique identification number allocated to each case.

Case Status

Case Status is the current state of a case. Status values used for the case are New, Pending, Escalated, or Closed. When a case is created, the status is set to New by default.

Case Type

Type of case.

- CSR - CSR cases are used in customer care situations associated within the normal course of doing business online and over the phone when providing assistance to customers. A CSR case is attached to a user.
- Agent - Agent cases that fraud investigators and investigation managers work on. They are used specifically by fraud investigators and investigation managers for analyzing data and finding relationships between sessions and cases. An Agent case is not attached to any user like a CSR case.

Cases

Case tools for servicing customer needs. Tools enables the institution to review servicing logs for each individual client to investigate the reasons that actions were taken or alerts were triggered.

Challenge Questions

Challenge Questions are a finite list of questions used for secondary authentication.

Configurable Actions

Configurable Actions allow a user to create new supplementary actions that occur after the running of rules.

Completed Registration

Status of the user that has completed registration. To be registered a user may need to complete all of the following tasks: Personalization (image and phrase), registering KBA questions/answers and email/cellphone.

Cookie

A cookie (also browser cookie, computer cookie, tracking cookie, web cookie, internet cookie, and HTTP cookie) is a small string of text stored on a user's computer by a web browser. A cookie consists of one or more name-value pairs containing bits of information such as user preferences, shopping cart contents, the identifier for a server-based session, or other data used by Web sites. It is sent as an HTTP header by a web server to a web client (usually a browser) and then sent back unchanged by client each time it accesses that server. A cookie can be used for authenticating, session tracking (state maintenance), and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts.

Creation Method (Buckets)

- Single Bucket - Single-bucket patterns will create and populate one bucket with the exact data points and value ranges specified in the pattern
- Multi- Bucket – Multi-bucket patterns have buckets for sub-ranges of a parameter range

CSR

Customer service representatives resolve low risk customer issues originating from customer calls. CSRs has limited access to Adaptive Risk Manager

- View the reason why a login or transaction was blocked
- View a severity flag with alert status to assist in escalation
- Complete actions such as issuing temporary allow for a customer

CSR Cases

CSR Cases are used in customer care situations associated within the normal course of doing business online and over the phone when providing assistance to customers. The customer support representatives can use the CSR set of tools for handling inquiries associated with Adaptive Risk Manager.

CSR Manager

A CSR Manager is in charge of overall management of CSR type cases. CSR Managers have all the access and responsibilities of a CSR plus access to more sensitive operations.

Date of Last Case Action

In cases, the date when last action occurred.

Date of Last Global Case Action

The last action performed against the user online.

Date of Last Online Action

Date when last online action was executed

Device

A computer, PDA, cell phone, kiosk, etc used by a user

Device Fingerprinting

A mechanism to recognize the device a customer typically uses to login – whether it is a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device. The fingerprinting process produces a fingerprint that is unique to the user and designed to protect against the "replay attacks" and the "cookie based registration bypass" process.

Disposition

The disposition describes the way in which the issue was resolved in a case. Cases only have dispositions when they're closed. If a case has any status besides closed, the disposition is left blank.

Device Registration

Device registration is a feature that allows a user to flag the device (computer, mobile, PDA, and others) he is using as a safe device. The customer can then configure the rules to challenge a user that is not coming from one of his registered devices.

Entities Editor

A tool to edit entities, a user-defined structure that can be re-used across different transactions. Only appropriate and related fields should be grouped into an Entity.

Entity

1. A referencible data structure that can be used in transaction definitions or directly in patterns. Entities or actors are users, devices, IP.

2. Entity can be defined as an organized array of individual elements and parts forming and working as a unit

3. Entity is a set of fields. It is like a user-defined structure that can be re-used across different transactions

Expiration Date

Date when CSR case expires. By default, the length of time before a case expires is 24 hours. After 24 hours, the status will change from New to Expired. After the case expires, the CSR user will not be able to open the case anymore, but the CSR Manager will be able to. The length of time before a case expires is configurable.

Evaluation Priority

The priority in which data is evaluated.

- First

  The data is evaluated in real-time (highest priority)

- Second

  The data is evaluated in near-real-time (low priority). If the server has a large system load, the patterns marked as "second" can be skipped. The system load is the number of authentication, transaction, rule processing (and other) reports and requests served by the Oracle Adaptive Access Manager server.

Fraud Investigator

A Fraud Investigator primarily looks into suspicious situations either escalated from customer service or directly from Adaptive Risk Manager alerts. Agents have access to all of the customer care functionality as well as read only rights to security administration and BI Publisher reporting.

Fraud Investigation Manager

A Fraud Investigation Manager has all of the access and duties of an investigator plus the responsibility to manage all cases. A manager must routinely search for overdue cases to make sure none are forgotten.

Fraud Scenario

A fraud scenario is a potential or actual deceptive situation involving malicious activity directed at a company's online application.

Gated Security

The multiple security checkpoints a user must pass through to gain access to sensitive data or transactions.

Groups

Groups allow you to view and administister a collection of like items as a single group. You should assign each group a unique name. The types of groups you can create include User ID, Login ID, Location, Device, Action, and Alert.

HTTP

Hypertext Transfer Protocol

IP address

Internet Protocol (IP) address

KBA Phone Challenge

When a customer's challenge questions are used for phone authentication. If the customer answers the question correctly, the system automatically takes appropriate action depending on their status such as unlocking the customer if they were locked out. If the customer answered the question incorrectly, they will get additional attempts at that question (depending on configuration). If the customer exceeds the maximum number of failures for a question another question will be asked. If two or more questions are asked in this process, and they answer successfully, their questions are automatically reset. If all of the questions were asked and the customer failed all attempts at each question, the customer will be locked out of online access.

KBA (Knowledge Based Authentication)

KBA is a secondary authentication infrastructure for pre-registered challenge questions, the creation, edit, validations, registration, presentation, and answers of challenge questions.

KeyPad

Virtual keyboard for entry of passwords, credit card number, and on. The KeyPad protects against Trojan or keylogging.

Keystroke Loggers

Software that captures a user's keystrokes. Keylogging software can be used to gather sensitive data entered on a user's computer.

Last Case Action

The last action executed in the CSR or Agent case.

Last Global Case Action

The last action that occurred for this user in all CSR cases. Agent cases and Escalated cases are not taken into account.

Last Online Action

The last action that user executed, for example - Answered challenge question would show "Challenge Question" or if user is blocked, "Block."

Location

A city, state, country, IP, network ID, etc from which transaction requests originate.

Locked

"Locked" is the status that Oracle Adaptive Access Manager sets if the user fails a question challenge. The "Locked" status is only used if the One-Time-Password (OTP) facility is in use. OTP sends a one-time password to the user via e-mail or SMS text message. If the user exceeds the number of retries when attempting to put in his OTP code, then his account becomes "Locked." After that, a Customer Service Representative must reset the status to "Unlocked" before the account can be used to enter the system.

Malware

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malware may contain key loggers or other types of malicious code.

Man-In-The-Middle-Attack (Proxy Attacks)

An attack in which a fraudster is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised

Manual Override

Outcomes based strictly on the combinations of Rule triggers. You can specify a score, action group and alert group based on different Rule return combinations or you can point to a nested models to further evaluate the risk. The rows of manual overrides evaluate from top to bottom, stopping as soon as a Rule return combination is matched. Actions and alerts triggered by a manual override will be added to any actions and alerts triggered by individual Rules.

Member

The member is the actor for which data needs to be captured.

Model

A Model is a set of rules that run at a single time. A Model contains rules that when linked to a group, are used to evaluate group members. The rules are added to the Model, configured, and linked to groups by the administrator. A new rule can be added to an existing Model at any time. In a Model, you can control the timing and combinations of rule firing with manual overrides.

Mutual Authentication

Mutual authentication or two-way authentication (sometimes written as 2WAY authentication) refers to two parties authenticating each other suitably. In technology terms, it refers to a client or user authenticating himself to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity.

Nested Models

A Nested Model is a secondary model used to further quantify the risk score in instances where the original result output by the system is inconclusive. Nested Models can be assigned to ensure a higher degree of accuracy for the risk score. A Nested Model is run only when a specific sequence of answers is returned from the primary Model. Nested Models therefore reduce false positives and negatives.

One-Time PIN/Password

Generation and delivery of a single use volatile credential. For example: Server generated, hand-held device, software generated, and so on. The purpose of a one-time pin/password (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a bank account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the pin/password, as is done with a one-time pin/password, this risk can be greatly reduced.

Oracle Adaptive Access Manager

A product to protect the enterprise and its customers online.

Out Of Band Authentication

The use of two separate networks working simultaneously to authenticate a user. For example: email, SMS, phone, and so on.

Overdue

A flag that will signal when a case has not been accessed in a given time range. The overdue flag is set to allow managers to see cases that require attention.

Patterns

A composite of traits or features characteristic of an individual or a group. One's pattern of behavior.

Used for Auto-learning, a profiling process in which an administrator defines behavior patterns. These patterns are in turn used by Adaptive Risk Manager to dynamically create and populate buckets based on the pattern parameters.

- An individual's location is from USA and from his home desktop
- The accounts group processes orders between 8AM-1PM
- A user transfers amount between $100 to $200 once a week to his overseas account

Personalization Active

Status of the user who has an image, a phrase and questions active. Personalization consists of a personal background image and phrase. The timestamp is generated by the server and embedded in the single-use image to prevent reuse. Each Authenticator interface is a single image served up to the end user for a single use.

Pharming

Pharming (pronounced farming) is an attack aiming to redirect a Web site's traffic to another, bogus Web site.

Phishing

A criminal activity utilizing social engineering techniques to trick users into visiting their counterfeit Web application. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity. Often a phishing exercise starts with an email aimed to lure in gullible users.

PinPad

Authentication entry device used to enter a numeric PIN.

Plug-in

A plug-in consists of a computer program that interacts with a host application (a web browser or an email client, for example) to provide a certain, usually very specific, function "on demand".

Policy Set

A policy set is the collection of all the currently configured policies used to evaluate traffic to identify possible risks. As a fail-safe, an action override or a score override can be created for a policy set so that the override is automatically invoked to override a particular action triggered by a rule when a specific set of circumstance occurs.

Policy Type

The Policy Types are Security and Business.

- Security Policy-A Security Policy is based on cross-industry best practices.
- Business Policy-A Business Policy is based upon parameters established for mitigation of transaction risk

Risk Score

The numeric risk level associated with a Runtime.

Questions Active

Status of the user who has completed registration and questions exists by which he can be challenged.

QuestionPad

Device that presents challenge questions for users to answer before they can perform sensitive tasks. This method of data entry helps to defend against session hijacking.

Rule Conditions

Rule conditions are the building blocks and make the rule-related functions in Oracle Adaptive Access Manager available to the client.

Rules

Rules are housed in Models, identify and react to certain information, and trigger actions, alerts, and scores. Rules can be added to Models, and Models can be applied to a group of users or all users.

Runtime

A Runtime is a specified point in a session when rules in a model will run. For example, at pre-authentication, post-authentication, and in-session. Risk can be evaluated at any time specified by a Runtime. To gain access to sensitive data or transactions a user must successfully pass through multiple security checkpoints.

Scores & Weights

Score refers to the numeric scoring used to evaluate the risk level associated with a specific situation. Weight refers to the multiplier used to influence the total score at various evaluation levels. Weight is only applied to a score when a given Model or Policy type is using a "weighted" scoring engine.

Scoring Engine

Fraud analytics engine you want to use to calculate the numeric score that determines the risk level. The various engines are listed below along with examples of how each scoring engine would calculate a Model Score.

- Aggregate Score

  Sum of the scores of all fired Rules.

- Average

  Average = (sum of scores of all fired Rules) / (count of all Rules used)

- Maximum

  Higher score out of all fired Rules

- Minimum

  Lower score out of all fired Rules

- Weighted Average

  [Average =(sum of scores of all fired Rules) / (count of all Rules used)] * (weight modifier specified by Model)

- Weighted Maximum Score

  (larger score out of all fired Rules) * (weight modifier specified by Model)

- Weighted Minimum Score

  (lower score out of all fired Rules) * (weight modifier specified by Model)

Restricted Note

A note describing why an action was taken in a case. A "Restricted" note can only be written by investigators and read by customer service managers and investigators.

Security Token

Security tokens (or sometimes a hardware token, hard token, authentication token, USB token, cryptographic token) are used to prove one's identity electronically (as in the case of a customer trying to access their bank account). The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something.

Severity Level

A marker to communicate to case personnel how severe this case is. The severity level is set by whomever creates the case. The available severity levels are High, Medium, and Low. If a customer suspects fraud, then the severity level assigned is "High." If the customer wants a different image, then the severity level assigned is "Low." Severity levels of a case can be escalated or de-escalated as necessary.

Session Hijacking

The term Session Hijacking refers to the exploitation of a valid computer session - sometimes also called a session key - to gain unauthorized access to information or services in a computer system

SOAP

SOAP, originally defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) as its message format, and usually relies on other Application Layer protocols (most notably Remote Procedure Call (RPC) and HTTP) for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.

Social Engineering

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information to a fraudulent entity.

Spoofing Attack

In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Spyware

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

Standard Note

A note describing why an action was taken in a case. A "Standard" note can be written and read by customer service representatives, managers, and investigators.

Status (Pattern)

Status is the current state of a Pattern.

- Active - If data needs to be collected, the pattern must be in the active state.
- Inactive - If the pattern is complete, but you don't want to collect data, pick "Inactive."
- Incomplete - If pattern creation has started, but you need to save it for completion later, choose "Incomplete." Data is not collected for this state.
- Invalid - The administrator may choose to mark the pattern as invalid if he does not want the pattern used. Data is not collected for this state.

Strong Authentication

An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security

constraints. Two-factor authentication (T-FA) is a system wherein two different factors are used in conjunction to authenticate. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance.

Using more than one factor is sometimes called strong authentication.

Temporary Allow

Temporary account access that is granted to a customer who is being blocked from logging in or performing a transaction.

Temporary Allow Active

Temporary allow is active.

Temporary Allow Expiration Date

Date when temp allow expires.

TextPad

Personalized device for entering a password or PIN using a regular keyboard. This method of data entry helps to defend against phishing.

Transaction Definition

Application data is mapped using the transaction definition before transaction monitoring and profiling can begin. Each type of transaction Oracle Adaptive Access Manager deals with should have a separate transaction definition.

Trojan/Trojan Horse

A program that installs malicious software while under the guise of doing something else.

User

A business, person, credit card, etc that is authorized to conduct transactions.

Virus

A computer program that can copy itself and infect multiple computers without permission or knowledge of the users.

Index

A

B

C

D

E

F

G

I

K

L

M

N

O

P

Q

R

S

T

U

W